GFI EventsManager 8

Handbuch

GFI Software Ltd.

http://www.gfisoftware.de
E-Mail: info@gfisoftware.de

Dieses Handbuch wurde von GFI Software Ltd verfasst und produziert. Die Informationen in diesem Dokument können ohne vorherige Ankündigung geändert werden. In den Beispielen verwendete Firmen, Namen und Daten sind, sofern nicht anders angegeben, rein fiktiv. Ohne vorherige ausdrückliche und schriftliche Zustimmung von GFI Software Ltd. darf das Dokument weder ganz noch teilweise in irgendeiner Form, sei es elektronisch oder mechanisch, oder zu irgendeinem Zweck reproduziert bzw. übertragen werden.

GFI EventsManager wurde von GFI Software Ltd. entwickelt. GFI EventsManager ist von GFI Software Ltd. urheberrechtlich geschützt. © 2000-2008 GFI Software Ltd. Alle Rechte vorbehalten.

Version 8 – Letzte Aktualisierung: 08.05.08

Inhaltsverzeichnis

Einführung 5

Informationen zu diesem Handbuch 5
Aufbau dieses Handbuchs 5
Definitionen der in diesem Handbuch verwendeten Begriffe 6
Über GFI EventsManager 8
Hauptmerkmale 9
Funktionsweise von GFI EventsManager 12
Module mit erforderlichen administrativen Zugriffsrechten 13
Die Verwaltungskonsole von GFI EventsManager im Überblick 14
Lizenzierung 15

Installation 17

Einführung 17
Installieren von GFI EventsManager in einem Local Area Network (LAN) 18
Installieren von GFI EventsManager in einer demilitarisierten Zone (DMZ) 19
Verwalten von Ereignissen von Microsoft Windows Vista und Windows Server 2008 20
Hardware-Anforderungen 20
Software-Anforderungen 21
Aktualisieren einer früheren Version 21
Starten der Installation 21

Erste Schritte 25

Einführung 25
Erste Schritte: Starten von GFI EventsManager 29
Erste-Schritte-Dialog 29
Konfigurieren des Datenbank-Backends 30
Konfigurieren der SQL Server-Einstellungen 31
Konfigurieren des Administratorkontos von GFI EventsManager 32
Konfigurieren allgemeiner Optionen für Warnungen 37
Konfigurieren von E-Mail-Warnungen 38
Konfigurieren von Warnungen per Netzwerknachricht 38
Konfigurieren von SMS-Warnungen 39
Ändern der allgemeinen Optionen für Warnungen 40
Erste Schritte: Verarbeiten von Ereignisprotokollen 41

Konfigurieren von Ereignisquellen 43

Einführung 43
Hinzufügen neuer Ereignisquellen zu einer Gruppe der „Computers Groups“ 43
Konfigurieren der Eigenschaften einer Ereignisquelle 45
Festlegen allgemeiner Eigenschaften einer Ereignisquelle 46
Festlegen alternativer Anmeldeinformationen des Domänenadministrators 46
Konfigurieren der üblichen Betriebszeit einer Ereignisquelle 47
Festlegen von Einstellungen für die Ereignisverarbeitung 48

Hinzufügen einer neuen SQL-Server-Gruppe 49
Festlegen der Eigenschaften von SQL-Servern als Ereignisquelle 49
Erweitern der Standardgruppe um neue SQL-Server 50
Entfernen von SQL-Servern aus der Standardgruppe 52
Festlegen der Eigenschaften eines SQL-Servers 52

Erstellen von Regeln zur Ereignisverarbeitung 55

Einführung 55
Erfassen und Verarbeiten von Windows-Ereignisprotokollen 57
Konfigurieren individueller Ereignisprotokolle 61
Erfassen und Verarbeiten von W3C-Protokollen 62
Erfassen und Verarbeiten von Syslog-Meldungen 64
Konfigurieren des Syslog-Server-Ports 66
Erfassen und Verarbeiten von SNMP-Traps 68
Konfigurieren der Einstellungen des SNMP-Trap-Servers 71
Archivieren von Ereignissen 72
Auswählen von Regeln zur Ereignisverarbeitung 73
Manuelles Scannen von Ereignisquellen 74

Konfigurieren von Warnungen und Aktionen 75

Einführung 75
Konfigurieren der standardmäßigen Klassifizierungsaktionen 76
Konfigurieren von Aktionen für Regeln zur Ereignisverarbeitung 77

Ereignisanzeige per Events-Browser 79

Einführung 79
Anzeigen gespeicherter Ereignisprotokolle 83
Starten einer Ereignisabfrage 84
Erstellen benutzerdefinierter Ereignisabfragen 85
Anpassen des Ereignisanzeige-Bereichs 86
Farbliches Kennzeichnen von Ereignissen 88
Tool zur Ereignissuche 89
Tool zum Export von Ereignissen 90
Sichern von Ereignissen 91
Wechseln zwischen Datenbanken 91
Löschen aller Ereignisse 91

Statusüberwachung 93

Einführung 93
Aufrufen des Status-Monitors 93
Ansicht zum allgemeinen Status („General“) 94
Ansicht zu Erfassungsabläufen („Job Activity“) 97
Ansicht zu Statistiken („Statistics“) 100

Datenbankoperationen 103

Einführung 103
Gründe für die Datenbankwartung 103
Konfigurieren der Datenbankwartung per Database Operations 105
Einrichten einer Wartungsaufgabe 107
Aufgabe „Move to database“ (in Datenbank verschieben) 110
Aufgabe „Export to file“ (in Datei exportieren) 111
Aufgabe „Import from file“ (aus Datei importieren) 113
Aufgabe „Delete data“ (Daten löschen) 115
Konfigurieren der Datenfilter-Bedingungen 116
Anzeigen geplanter Wartungsaufgaben 118
Bearbeiten einer Wartungsaufgabe 119
Ändern der Priorität einer Wartungsaufgabe 120

Löschen einer Wartungsaufgabe 120

Anpassen von Regeln zur Ereignisverarbeitung 121

Einführung 121
Erstellen eines neuen Regelsatz-Ordners 122
Umbenennen und Löschen von Ordnern 122
Erstellen eines neuen Regelsatzes 123
Bearbeiten eines Regelsatzes 123
Löschen eines Regelsatzes 124
Erstellen einer neuen Regel für Windows-Ereignisprotokolle 124
Erstellen einer neuen Regel für W3C-Protokolle 127
Erstellen einer neuen Syslog-Regel 130
Erstellen einer neuen Regel für SNMP-Traps 132
Erstellen einer neuen Regel für SQL-Server-Audit-Protokolle 135
Ändern der Eigenschaften einer Regel 138
Festlegen erweiterter Einstellungen zur Ereignisfilterung 139
Bedingungen für Windows-Ereignisse 139
Syslogspezifische Kategorien 139

Konfigurieren von Benutzern und Gruppen 141

Einführung 141
Erstellen eines neuen Benutzers 141
Ändern von Benutzereigenschaften 142
Löschen von Benutzern 143
Konfigurieren einer Benutzergruppe 143
Ändern von Eigenschaften einer Benutzergruppe 144
Löschen von Benutzergruppen 144
Aktivieren/Deaktivieren der Anmeldung bei GFI EventsManager 145
Aktivieren/Deaktivieren der Überwachung von Benutzeraktionen 146

Weiterführende Optionen 149

Befehlszeilen-Tools 149
Lizenzierung 152
Eingeben des Registrierschlüssels nach der Installation 152
Versionsinformationen 153
Suchen nach neueren Builds 153

Fehlerbehebung 155

Einführung 155
Knowledge-Base 155
Web-Forum 155
Technischer Support von GFI 155
Benachrichtigung bei neuen Builds 156

Index 157

Einführung

Informationen zu diesem Handbuch

Aufbau dieses Handbuchs

In diesem Handbuch werden alle aufeinander aufbauenden Schritte beschrieben, die erforderlich sind, um GFI EventsManager zu installieren, einzurichten und zu verwenden.

Kapitel 1 präsentiert einen Überblick über die Funktionsweise von GFI EventsManager.

Kapitel 2 erläutert die Installation von GFI EventsManager.

Kapitel 3 befasst sich mit der Festlegung der wichtigsten Parameter, die für den ersten Start des Programms erforderlich sind. Alle notwendigen Einstellungen werden Schritt für Schritt erklärt.

Kapitel 4, 5 und 6 helfen Ihnen bei der Konfigurierung grundlegender Einstellungen zur Ereignisverarbeitung. Mit den in diesen Kapiteln präsentierten Informationen ist es Ihnen möglich:

- Zu überwachende Ereignisquellen zu bestimmen (z. B. SQL Server)
- Zu erfassende und zu verarbeitende Protokolltypen (Windows-Ereignisse, W3C, Syslog, SNMP-Traps) festzulegen
- Regeln zur Ereignisverarbeitung einzurichten, die auf erfasste Protokolle angewendet werden
- Warnungen und Aktionen für wichtige Ereignisse einzurichten

Hinweis: Mit den Informationen dieser Kapitel besitzen Sie ausreichende Kenntnisse, GFI EventsManager anhand der standard-mäßigen Einstellungen zu betreiben.

Kapitel 7 erklärt, wie der integrierte Events Browser zur Analyse von Ereignissen zu verwenden ist, die im Datenbank-Backend von GFI EventsManager gesichert sind. Erfahren Sie, wie folgende Tools und Funktionen des Events Browser eingesetzt werden:

- Standardmäßige Ereignisprotokoll-Abfragen und der Abfrage-generator für benutzerdefinierte Vorgaben
- Farbliche Hervorhebung unterschiedlicher Ereignisse
- Tool zur Ereignissuche

Kapitel 8 erläutert, wie der Status-Monitor zur Kontrolle des Programmstatus' sowie zur Darstellung statistischer Informationen und verarbeiteter Ereignisse verwendet wird.

Kapitel 9 führt Sie durch die Erstellung und Anpassung von Regeln zur Ereignisverarbeitung. Dieses Kapitel richtet sich an erfahrene Anwender, die eigene Verarbeitungsregeln erstellen möchten.

Kapitel 10 befasst sich mit der Festlegung der Benachrichtigungseinstellungen für Warnungen an Systemverantwortliche:

- Persönliche Angaben der Empfänger, z. B. zur Mobilfunknummer.
- Normale Geschäftszeiten (Kernarbeitszeit)
- Art der an jeden Empfänger zu verschickenden Warnung

Kapitel 11 informiert über verschiedene Kontaktmöglichkeiten bei Fragen zur Problembehebung.

Definitionen der in diesem Handbuch verwendeten Begriffe

Aktionen	Schritte, die eingeleitet werden, wenn ein protokolliertes Ereignis zuvor festgelegte Bedingungen erfüllt. Beispielsweise lassen sich Aktionen durchführen, wenn ein Ereignis als kritisch eingestuft wurde. Unterstützt werden Aktionen wie der Versand von E-Mail-Warnungen, eine Ereignisarchivierung und die Ausführung von Skripten.
Warnungen	Informieren festgelegte Empfänger über den Eintritt eines bestimmten Ereignisses. GFI EventsManager kann Warnungen per E-Mail, SMS und Netzwerk verschicken.
Archiv	Enthält von GFI EventsManager im Microsoft SQL Server Datenbank-Backend gesicherte Ereignisse.
E-Mail-Warnung	Per E-Mail verschickte Benachrichtigung, die über den Eintritt eines bestimmten Ereignisses informiert. Erfordert den Zugriff auf einen aktiven E-Mail-Server.
Ereignisklassifizierung	Ereignisse werden von GFI EventsManager als kritisch, hoch, mittel, niedrig oder „Noise" (s. u.) eingestuft.
Ereignisprotokoll	Enthält Daten zu Ereignissen, die im Netzwerk oder auf einem Computer eingetreten sind. GFI EventsManager unterstützt die Erfassung unterschiedlicher Ereignisprotokolle: Windows-Ereignisprotokolle, W3C, Syslog, SNMP-Traps, SQL-Server-Überwachungsprotokolle).
Regeln zur Ereignis-verarbeitung	Legen fest, nach welchen Kriterien ein Ereignis-protokoll zu überprüfen ist.
Management Information Base	Eine Management Information Base (MIB) gleicht einem Datenbeschreibungsverzeichnis oder Code-Buch. Sie beschreibt Informationen (durch eindeutige Object Identifier, OIDs, identifizierte „Managed Objects" mit unterschiedlichen Parametern), die über ein Protokoll zur Netzwerkverwaltung abgefragt oder angepasst werden können. Der Zugriff auf in MIBs hierarchisch angeordnete Daten kann per SNMP erfolgen. Per MIB-gestützte Kontrolle lässt sich feststellen, ob z. B. ein SNMP-fähiges Netzwerkelement wie ein Router aktiv ist. Von diesen Elementen ausgegebene SNMP-Nachrichten werden verarbeitet und interpretiert.

Netzwerk-Warnung	Bezeichnet im Netzwerk verschickte Nachrichten (auch Net-Send-Nachrichten genannt), die über den Eintritt eines Ereignisses informieren. Diese Nachrichten werden mit Hilfe eines Instant-Messenger-System/Protokolls verschickt und über die Taskleiste des Empfängers angezeigt. Für Netzwerk-Warnungen müssen der Name oder die IP-Adresse des empfangenden Computers angegeben werden.
Noise („Rauschen“)	Bezeichnet sich wiederholende Protokolleinträge zu ein und demselben Ereignis.
Regelsatz-Ordner	Enthält einen oder mehrere Regelsätze.
Regelsatz	Zusammenstellung mehrerer Regeln zur Ereignisverarbeitung
SMS-Warnung	Per SMS verschickte Benachrichtigung, die über den Eintritt eines bestimmten Ereignisses informiert. SMS-Warnungen können unter anderem per Mobiltelefon (mit Modem) und Web-basierten E-Mail-to-SMS-Gateways verschickt werden.
SNMP-Object-Identifier (OID)	Gibt eine durch Punkte getrennte Ziffernkette an, mit der verwaltete Elemente (z. B. ein Router) eindeutig im Netzwerk identifiziert und lokalisiert werden (z. B. 1.3.6.1.4.1.2682.1). SNMP-OIDs sind ein wesentlicher Bestandteil von SNMP-Nachrichten. Nachrichten ohne OID können von SNMP-Servern nicht korrekt interpretiert und verarbeitet werden. Viele Hersteller bieten eigene MIBs mit speziell für ihre Geräte konzipierten OIDs.
SNMP-Traps	Werden bei wichtigen Ereignissen wie Fehlfunktionen oder Sicherheitsverletzungen von aktiven Netzwerkelementen (z. B. Hubs, Routern und Bridges) als Benachrichtigungen/Warnungen an SNMP-Server ausgegeben. SNMP-Trap-Daten können Konfigurations-, Status- und statistische Informationen wie die Anzahl der bisherigen Gerätefehlfunktionen enthalten.
Syslog-Meldungen	Werden bei Eintritt wichtiger Ereignisse von UNIX- und Linux-Systemen als Benachrichtigungen/Warnungen an einen Syslog-Server ausgegeben. Syslog-Meldungen können von Workstations, Servern und aktiven Netzwerkelementen und -anwendungen wie Cisco-Routern und Cisco PIX-Firewalls ausgegeben werden, um z. B. Fehlfunktionen und Sicherheitsverletzungen zu protokollieren.
Nicht klassifizierte Ereignisse	Ereignisse, die keine der in den Regeln zur Ereignisprotokollierung festgelegten Bedingungen erfüllen.
W3C-Protokolle	Ein vom World Wide Web Consortium entwickeltes allgemeines Protokollformat. W3C-Protokolle sind textbasierte Flat-Files, die von Webservern, u. a. dem Microsoft Internet Information Server (IIS), zur Aufzeichnung Web-spezifischer Ereignisse verwendet werden.

Windows Ereignisprotokolle	Sammlung von Einträgen zu Ereignissen, die auf einem Computer mit Windows-Betriebssystem eingetreten sind.

Über GFI EventsManager

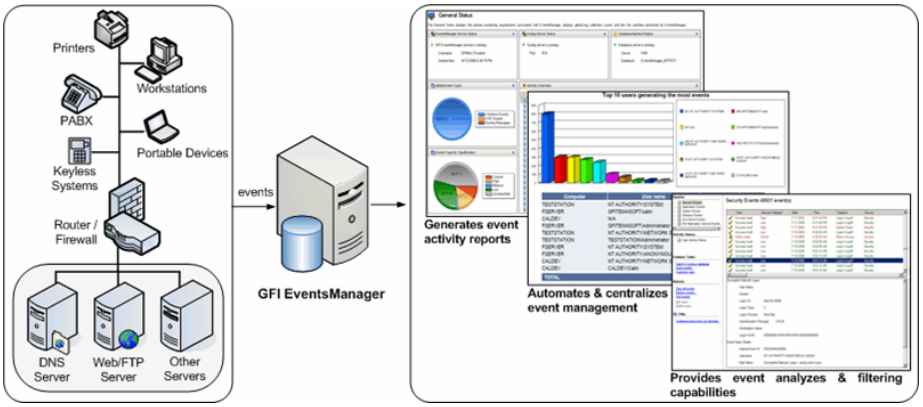


Abbildung 1 – Integration von GFI EventsManager mit jeder bestehenden IT-Infrastruktur

GFI EventsManager dient der zielgerichteten Verwaltung von Ereignisprotokollen und lässt sich in jede bestehende IT-Infrastruktur einbinden, um mit der Ereignisverwaltung verbundene Aufgaben im gesamten Netzwerk zu automatisieren und zu vereinfachen.

GFI EventsManager bietet folgende Leistungsmerkmale:

- Automatische Erfassung und zentrale Verwaltung von W3C-, Syslog- und Windows-Ereignissen sowie von SNMP-Traps, die von Netzwerkgeräten und Windows/Linux/Unix-basierten Systemen ausgegeben werden.
- Archivierung erfasster Ereignisse in einer zentralen SQL-Datenbank zwecks Analyse und forensischer Spurensuche.
- Filterung unerwünschter Ereignisse und Klassifizierung wichtiger Ereignisse durch leistungsfähige standardmäßige oder benutzer-definierbare Regeln zur Ereignisverarbeitung.
- Automatisierung der Ausgabe von Warnungen und der Einleitung von Gegenmaßnahmen bei Ereignissen mit hoher Dringlich-keitsstufe, beispielsweise durch Ausführung von Skripten und Dateien.
- Überwachung der Netzwerkaktivität und des Status der Scan-Engine von GFI EventsManager über eine integrierte Dashboard-Anzeige.
- Analyse von Ereignissen mit einem integrierten Events-Browser plus Export in CSV-Dateien zur weiteren Verarbeitung und Berichtanpassung.
- Vereinfachte forensische Spurensuche mit Hilfe von Spezial-werkzeugen wie dem integrierten Ereignisabfrage-Generator, einem Tool zur Ereignissuche und der farblichen Hervorhebung unterschiedlicher Ereignisse.
- Leistungsfähige Verarbeitung von Ereignissen per Hochleistungs-Scan-Engine.

- Erstellung, zeitgesteuerte Ausgabe und E-Mail-Versand von Trend-Reports zu Ereignisaktivitäten per GFI EventsManager ReportPack, dem im Lieferumfang von GFI EventsManager enthaltenen Reporting-Tool.
- Echtzeit-Überwachung des Betriebsstatus von SQL-Servern durch Verarbeitung der im Rahmen täglicher SQL-Server-Abläufe erstellten Aktivitätenprotokolle/Nachrichten.

Hauptmerkmale

Erweiterte Ereignisprotokoll-Unterstützung

GFI EventsManager verarbeitet verschiedene Arten von Ereignisprotokollen, darunter Windows-Ereignisprotokolle, W3C-Protokolle, Syslog-Meldungen und SNMP-Traps. Dank dieser umfangreichen Unterstützung lässt sich eine größere Auswahl an Daten unterschiedlicher Hardware- und Software-Lösungen erfassen, die am häufigsten in Unternehmensnetzwerken zu finden sind. Eine Übersicht zu Lösungen, deren Protokolle von GFI EventsManager standardmäßig unterstützt werden, erhalten Sie in diesem Knowledg-Base-Artikel von GFI: http://kbase.gfi.com/showarticle.asp?id=KBID003302.

Regelbasierte Verwaltung von Ereignisprotokollen

Nutzen Sie vorkonfigurierte Regeln zur Ereignisverarbeitung, mit denen Ereignisse aus verschiedenartigen Protokollen herausgefiltert und klassifiziert werden. Standardregeln lassen sich ohne weitere Konfigurierung einsetzen und darüber hinaus individuell verändern. Zudem können Sie neue, auf Ihre Netzwerkinfrastruktur zugeschnittene Regeln erstellen. Eine Übersicht zu Betriebssystemen und Geräten, für die GFI EventsManager vorkonfigurierte Verarbeitungsregeln bereitstellt, erhalten Sie in diesem Knowledge-Base-Artikel von GFI: http://kbase.gfi.com/showarticle.asp?id=KBID002868.

Scan-Profile für Ereignisprotokolle

Verwalten Sie Regeln zum Scannen von Ereignisprotokollen mit Hilfe von Scan-Profilen. Über ein Scan-Profil lassen sich gleich mehrere Regeln zur Ereignisprotokoll-Überwachung einrichten, die auf einen einzelnen Computer oder eine Computergruppe angewendet werden sollen. Die Vorteile von Scan-Profilen:

- Vereinfachung der Produktadministration durch zentrale Anpassung der Regeln zur Ereignisverarbeitung.
- Erstellung verschiedener Regelgruppen, die sich an die Funktion gescannter Ereignisquellen und die Netzwerkumgebung anpassen lassen. Regelgruppen können beispielsweise speziell auf die Arbeitsplatzrechner einer einzelnen Abteilung abgestimmt werden.

Granulare Regelkonfigurierung

Erstellen Sie ein übergreifendes Profil zur Ereignisverarbeitung, das für alle Computer gelten soll, und mehrere ergänzende Spezialprofile, die differenziertere Regeln für einzelne Computer enthalten.

Verständliche Erklärungen zu Windows-Ereignissen

Ein großer Nachteil der Ereignisprotokolle von Microsoft Windows ist die fehlende Benutzerfreundlichkeit, da Einträge nur schwer zu verstehen sind. Aus diesem Grund werden die Protokolle nur von wenigen Administratoren zur Kontrolle herangezogen. GFI EventsManager vereinfacht die Nutzung von Ereignisprotokollen, indem die Ereignisbeschreibungen in eine leicht verständliche Sprache übertragen werden.

Optimierte Event-Scan-Engine

Mit der leistungsfähigen Event-Scan-Engine von GFI EventsManager lassen sich Ereigniskontrollen schneller durchführen. Die flexibel erweiterbare Engine erlaubt es, zusätzliche Funktionen/Module hinzuzufügen, ohne Änderungen am eigentlichen Engine-Code vorzunehmen. Hierdurch wird mehr Stabilität erzielt, ohne die Skalierbarkeit zu beeinträchtigen.

Automatische Noise-Reduzierung

Unterwünschte Ereignisdaten (wie Noise oder von Hintergrundprozessen ausgegebene Ereignisse) werden erkannt und herausgefiltert, sodass Sie nur sicherheitsrelevante Informationen erhalten. Die somit reduzierte Anzahl der zu analysierenden Ereignisse erleichtert die forensische Spurensuche.

Aktionen in Echtzeit

Wird ein sicherheitsrelevantes Ereignis festgestellt, können Warnungen ausgegeben oder Aktionen durchgeführt werden, beispielsweise das Ausführen eines Skripts. Warnungen lassen sich auf unterschiedliche Weise an eine oder mehrere Personen verschicken: per E-Mail, Netzwerknachricht oder SMS-Mitteilung (über einen E-Mail-to-SMS-Gateway oder -Dienst). Aktionen können aufgrund der Ereignisklassifizierung oder durch bestimmte Bedingungen von Regeln zur Ereignisverarbeitung ausgelöst werden.

Fortschrittliche Funktionen zur Ereignisfilterung

GFI EventsManager bietet zahlreiche Funktionen zur Ereignisfilterung:

- **Vordefinierte Ereignisabfragen plus Abfrage-Generator für benutzerdefinierte Abfragen:** Mit Hilfe vordefinierter Ereignisabfragen können Daten aus Ereignisprotokollen so aufbereitet werden, dass nur gewünschte Ereignisse angezeigt werden – ohne dabei Einträge aus dem Datenbank-Backend zu löschen. Der integrierte Ereignisabfrage-Generator erlaubt das Erstellen eigener Ereignisabfragen.
- **Farbliche Hervorhebung unterschiedlicher Ereignisse:** Lassen Sie unterschiedliche Ereignisarten farblich kennzeichnen. Bei der Durchsicht von Protokollen werden wichtige Ereignisse somit leichter erkannt.
- **Tool zur Ereignissuche:** Durch Angabe von Suchkriterien wie dem Ereignistyp lassen sich wichtige Ereignisse schnell auffinden.

Zentralisierte Ereignisüberwachung und -verwaltung

Von Windows/Linux/UNIX-Systemen, Netzwerkgeräten und Software-Anwendungen ausgegebene Ereignisse lassen sich mit einer einzigen Benutzerkonsole überwachen und verwalten.

Benutzerspezifische Zugriffsrechte

Legen Sie differenziert fest, in welchem Umfang ein Zugriff auf die Verwaltungskonsole von GFI EventsManager möglich sein soll. Beispielsweise kann einigen berechtigten Anwendern nur die Anzeige von Ereignissen gestattet sein, während andere auch die Konfigurationseinstellungen von GFI EventsManager ändern dürfen.

SQL-Server-Überwachung

Lassen Sie GFI EventsManager den Betriebsstatus Ihrer SQL-Server automatisch überwachen. Die im Rahmen täglicher SQL-Server-Abläufe erstellten Aktivitätenprotokolle/Nachrichten werden hierfür in Echtzeit verarbeitet. Eine Überwachung erfolgt für Server-Start, Anmeldevorgänge, Backups, Server-seitige Ablaufverfolgungen u. Ä. Zudem kann GFI EventsManager bei wichtigen Ereignissen wie dem Herunterfahren des Servers oder mehreren nacheinander fehlgeschlagenen Anmeldungen Warnungen per E-Mail, Netzwerknachricht oder SMS-Mitteilung verschicken.

Modul Database Operations (WAN-Connector))

Ereignisinformationen, die von mehreren, im gesamten Netzwerk verteilten GFI EventsManager-Instanzen erfasst und verarbeitet wurden, lassen sich mit dem Modul „Database Operations" in einer Datenbank zentralisieren. Das Zusatzmodul vereinfacht zudem ein schnelles Backup und Wiederherstellen von Ereignissen. Darüber hinaus kann die Größe der Datenbank im Rahmen der automatischen Wartung durch den Export von Ereignissen reguliert werden.

Management Information Base

Viele Hersteller bieten für ihre Hardware Management-Information-Base-Dateien (MIBs) an, die spezielle Eigenschaften ihrer Geräte beschreiben. GFI EventsManager wird mit MIB-Definitionen folgender Hersteller ausgeliefert: Cisco, 3Com, IBM, HP, Check Point, Alcatel, Dell, Netgear, SonicWall, Juniper Networks, Arbor Networks, Oracle, Symantec, Allied Telesis u. a. Der MIB-Baum lässt sich zudem mit GFI EventsManager bearbeiten.

Unterstützung von Microsoft Windows Vista und Windows Server 2008

GFI EventsManager ist offiziell für Microsoft Windows Server 2008 zertifiziert, unter Windows Vista lauffähig und erfasst Ereignisse dieser Plattformen. Weiterhin unterstützt werden Microsoft Windows 2000, XP und 2003.

Funktionsweise von GFI EventsManager

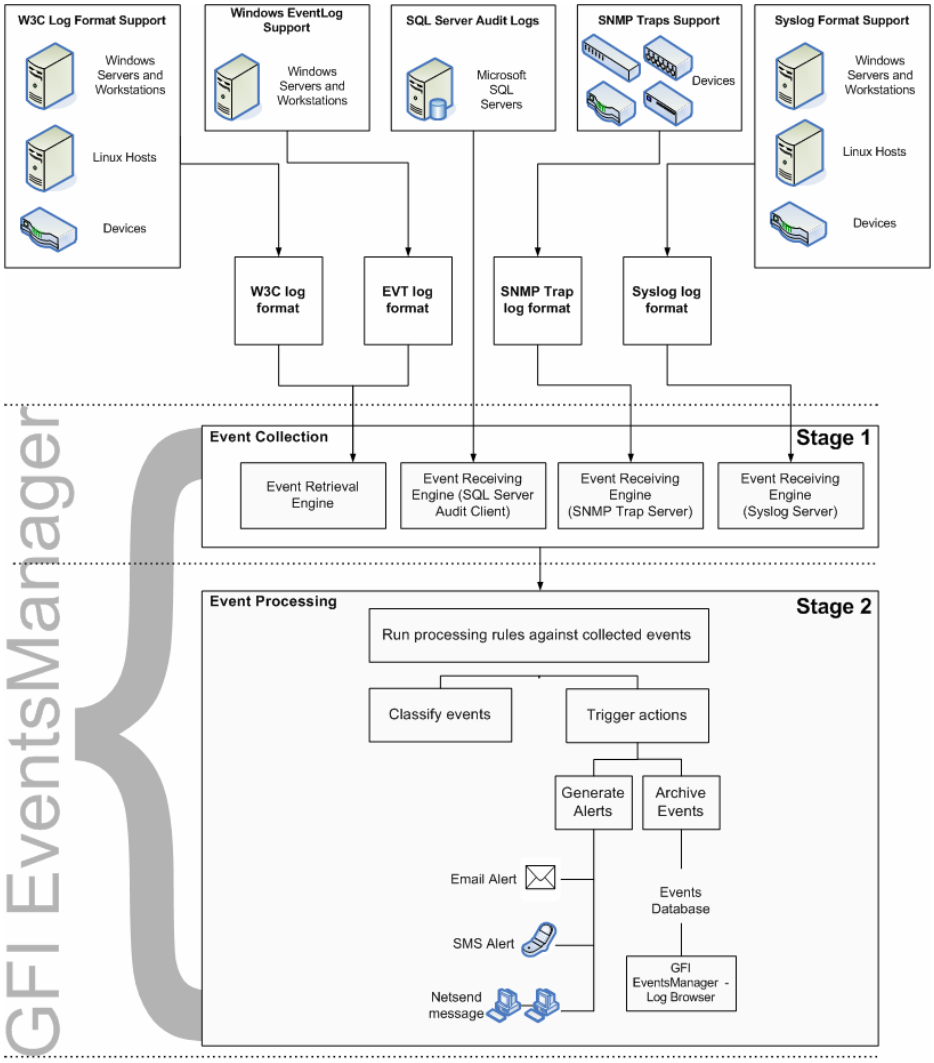


Abbildung 2 – Arbeitsabläufe von GFI EventsManager

GFI EventsManager bearbeitet Ereignisse in zwei Phasen:

- **Phase 1: Ereigniserfassung**
- **Phase 2: Ereignisverarbeitung**

Nachfolgend werden die Arbeitsabläufe der beiden Phasen beschrieben.

Phase 1: Ereigniserfassung

Während der Ereigniserfassung ruft GFI EventsManager Protokolle von verschiedenen Ereignisquellen ab. Hierfür stehen 2 Engines zur Verfügung: die Event Retrieval Engine und die Event Receiving Engine.

Die Event Retrieval Engine – Diese Engine wird zum Abruf der Windows-Ereignisprotokolle und W3C-Protokolle von Ereignisquellen im Netzwerk verwendet. Sie führt während der Ereigniserfassung folgende Schritte durch:

1. Anmeldung an der/den Ereignisquelle(n)
2. Erfassung von Ereignissen dieser Quelle(n)

3. Übermittlung der Ereignisse an den GFI EventsManager Server
4. Abmeldung von der/den Ereignisquelle(n)

Die Event Retrieval Engine erfasst Ereignisse in bestimmten Zeitabständen, die über die Verwaltungskonsole von GFI EventsManager konfigurierbar sind.

Die Event Receiving Engine – Diese Engine fungiert als Syslog-und SNMP-Trap-Server. Sie überwacht und erfasst Syslog-Ereignisse/Nachrichten und SNMP-Traps, die von unterschiedlichen Quellen im Netzwerk verschickt wurden. Im Gegensatz zur Event Retrieval Engine empfängt die Event Receiving Engine Nachrichten direkt von der Ereignisquelle. Eine Remote-Anmeldung vor dem Erfassen von Ereignissen ist in diesem Fall nicht erforderlich. Syslog-Ereignisse/Nachrichten und SNMP-Traps werden zudem in Echtzeit erfasst, daher müssen keine Abruf-Intervalle definiert werden.

Die Event Receiving Engine überwacht Syslog-Meldungen auf Port 514 und SNMP-Traps auf Port 162. Diese Einstellungen können jedoch über die Verwaltungskonsole von GFI EventsManager geändert werden.

Phase 2: Ereignisverarbeitung

Während dieser Phase überprüft GFI EventsManager die erfassten Ereignisse mit Hilfe mehrerer Regeln zur Ereignisverarbeitung. Sie bewirken, dass

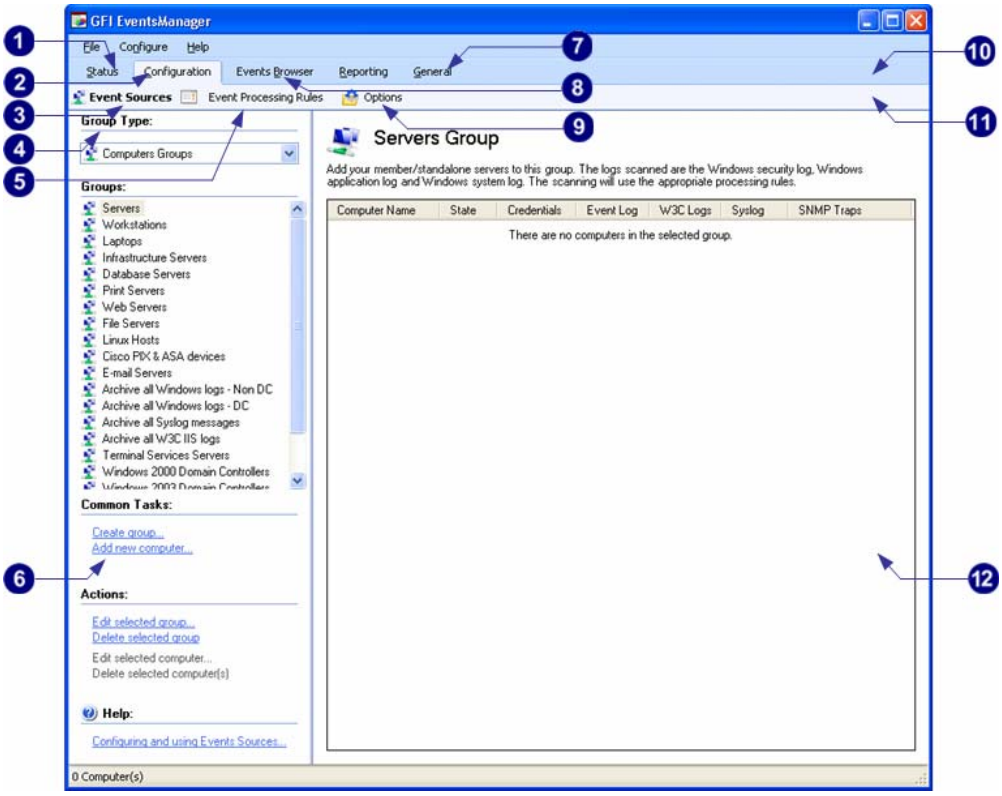
- erfasste Protokolle analysiert und kontrollierte Ereignisse als kritisch, hoch, mittel, niedrig oder „Noise“ klassifiziert werden,
- Ereignisse, die bestimmten Kriterien entsprechen, herausgefiltert werden,
- bei wichtigen Ereignissen Warnungen per E-Mail, SMS und Netzwerk versendet werden,
- bei wichtigen Ereignissen Aktionen eingeleitet werden, wie die Ausführung von exe-Dateien oder Skripten, und dass
- erfasste Ereignisse im Datenbank-Backend archiviert werden (optional).

GFI EventsManager kann darüber hinaus Ereignisse ohne die vorherige Kontrolle durch Regeln archivieren. In diesem Fall erfolgt die Archivierung ebenfalls im Rahmen der der Ereignisverarbeitung.

Module mit erforderlichen administrativen Zugriffsrechten

Zur Verwendung einiger Hauptmodule von GFI EventsManager sind Administratorrechte erforderlich. Weitere Informationen zu diesen Modulen erhalten Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID001122.

Die Verwaltungskonsole von GFI EventsManager im Überblick



Screenshot 1 – Verwaltungskonsole von GFI EventsManager

1. **Status** – Mit Hilfe dieser Option können Sie den Programmstatus von GFI EventsManager und statistische Daten zu verarbeiteten Protokollen abrufen.
2. **Configuration** – Hierüber können Sie die wichtigsten Funktionen zur Ereignisverarbeitung aufrufen und bearbeiten.
3. **Event Sources** – Legen Sie mit Hilfe dieser Option Ereignisquellen fest sowie welche Protokolle zu erfassen und welche Regeln zur Ereignisverarbeitung anzuwenden sind.
4. **Group Type** – Wechseln Sie zwischen den Gruppen „Computer“ und „Datenbank-Server“ als Quellen für Ereignisprotokolle.
5. **Event Processing Rules** – Mit dieser Option können Sie Regeln zur Ereignisverarbeitung erstellen, bearbeiten und individuell anpassen.
6. **Common Tasks** – Im linken Fensterbereich können Sie zusätzliche Konfigurationsoptionen von GFI EventsManager aufrufen.
7. **General** – Mit dieser Option können Sie nach Produkt-Updates suchen sowie Informationen zur Produktversion und Lizenzierung abrufen.
8. **Events Browser** – Mit dieser Option können Sie die im Datenbank-Backend von GFI EventsManager gespeicherten Ereignisse anzeigen.
9. **Options** – Mit dieser Option können Sie allgemeine Einstellungen vornehmen, z. B. zum Datenbank-Backend und

zu Warnungen.

10. Greifen Sie über die Reiter dieser Leiste auf die wichtigsten Konfigurationsoptionen von GFI EventsManager zu.
11. Legen Sie über die Optionen dieser Leiste die einzelnen Betriebsparameter von GFI EventsManager fest.
12. Bereich zur Ereignisanzeige und Festlegung von Parametern.

Lizenzierung

Beim Einsatz der Testversion von GFI EventsManager stehen alle Leistungsmerkmale der Vollversion zur Verfügung. Sie können die Software standardmäßig 10 Tage lang uneingeschränkt testen. Durch Eingabe eines 30-Tage-Registrierschlüssels lässt sich die Testdauer auf insgesamt 30 Tage verlängern. Der 30-Tage-Registrierschlüssel wird an die E-Mail-Adresse geschickt, die Sie vor dem Download des Produkts auf der GFI-Website angegeben haben.

Um GFI EventsManager nach Ablauf des Testzeitraums weiter nutzen zu können, müssen Sie einen kostenpflichtigen Registrierschlüssel erwerben. Informationen zu den Lizenzoptionen finden Sie auf der Website von GFI unter: http://www.gfi.com/pricing/pricelist.aspx?product=esm&curr=eur&lang=de. Zur Verwendung von GFI EventsManager ist immer nur ein Registrierschlüssel erforderlich. Der Umfang der nutzbaren Funktionen richtet sich nach dem von Ihnen erworbenen Schlüsseltyp.

Hinweis: Zur dauerhaften Verwendung des Produkts ist lediglich der neue Registrierschlüssel einzugeben, eine De- und Neuinstallation des Produkts ist nicht erforderlich.

Installation

Einführung

Wo kann GFI EventsManager im Netzwerk installiert werden?

GFI EventsManager kann ungeachtet ihres Standorts auf allen Computern im Netzwerk installiert werden, die die Systemvoraussetzungen erfüllen.

Es lassen sich Ereignisse verwalten, die erzeugt worden sind auf

- dem Computer, auf dem GFI EventsManager installiert wurde,
- auf allen Computern, auf die der Computer mit GFI EventsManager zugreifen kann.

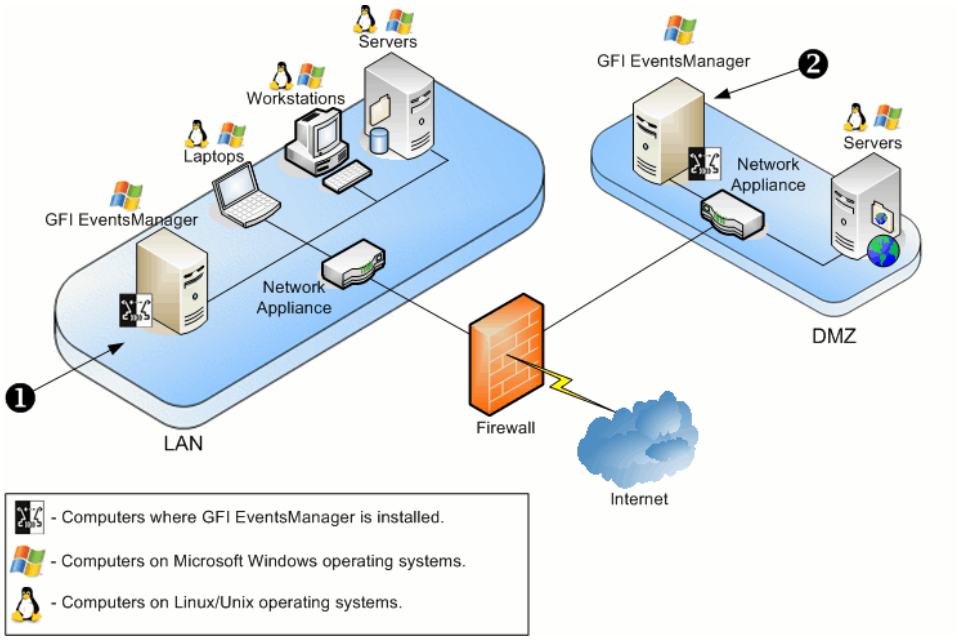


Abbildung 3 – Installationsmöglichkeiten von GFI EventsManager

GFI EventsManager lässt sich wie folgt installieren:

❶ Innerhalb des Netzwerks, um die Aktivitäten interner Server und Workstations/Endpunkte zu überwachen.

❷ In der DMZ, um auf Ihren Servern erzeugte Ereignisse zu überwachen und zu verwalten

Installieren von GFI EventsManager in einem Local Area Network (LAN)

GFI EventsManager kann in Windows-basierten Netzwerken und gemischten Umgebungen mit Linux- und UNIX-Systemen installiert werden.

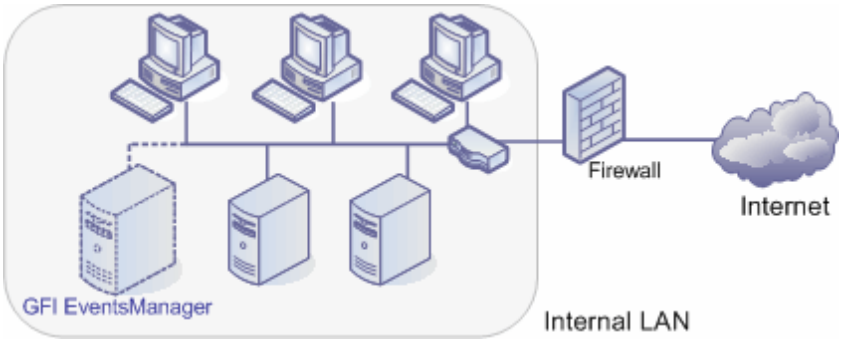


Abbildung 4 – Installation von GFI EventsManager in einem LAN

Bei der LAN-Installation von GFI EventsManager lassen sich Windows-Ereignisse, W3C-Protokolle, Syslog-Meldungen, SNMP-Traps und SQL-Server-Ereignismeldungen verwalten, die von mit dem LAN verbundener Hard- oder Software ausgegeben werden, darunter:

- Workstations und Server (z. B. Apache Webserver)
- Netzwerk-Hardware (z. B. Cisco PIX-Firewalls)
- Software von Drittanbietern
- spezielle Dienste (z. B. Microsoft Internet Information Server, IIS)
- Telefonanlagen, schlüssellose Zugangskontrollen, Intrusion-Detection-Systeme (IDS) u. Ä.

Bei einer LAN-Installation lässt sich GFI EventsManager zudem zum Erfassen von Ereignissen verwenden, die von Hard- und Software in einer demilitarisierten Zone (DMZ) stammen. Hierfür sind jedoch folgende Voraussetzungen zu erfüllen, da die DMZ für gewöhnlich durch eine Firewall oder einen Router geschützt wird:

1. Die von GFI EventsManager verwendeten Ports dürfen nicht von der Firewall blockiert werden. Weitere Informationen hierzu erhalten Sie in folgendem Knowledge-Base-Artikel von GFI: http://kbase.gfi.com/showarticle.asp?id=KBID002770.

2. GFI EventsManager muss administrative Zugriffsrechte auf die in der DMZ laufenden Computer besitzen.

Installieren von GFI EventsManager in einer demilitarisierten Zone (DMZ)

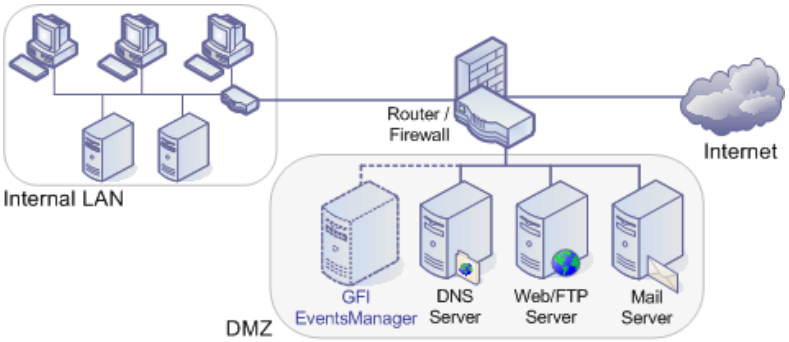


Abbildung 5 – Zwischen dem internen LAN und dem Internet eingerichtete DMZ

GFI EventsManager lässt sich auch in einer demilitarisierten Zone (DMZ) installieren. Dieses neutrale, geschützte Netzwerk befindet sich zwischen dem internen Unternehmensnetzwerk (LAN) und externen Netzen wie dem Internet. Bei dieser Installationsvariante lässt sich die Verwaltung von Ereignissen, die von in der DMZ eingerichteten Hardware und Software erzeugt werden, ebenfalls automatisieren.

Automatisieren der Verwaltung von Web- und Mailserver-Ereignissen

DMZ-Netzwerke werden üblicherweise für Hardware und Software eingerichtet, die mit dem Internet kommuniziert, z. B. HTTP-, FTP- und Mailserver.

GFI EventsManager unterstützt die automatische Verwaltung von Ereignissen folgender Server:

- Mit Linux/Unix betriebene Webserver, inklusive der Ereignisse aus W3C-Protokollen von Apache-Webservern auf LAMP-Web-Plattformen
- Windows-basierte Webserver inklusive der von den Microsoft Internet Information Services (IIS) erzeugten W3C-Protokolle
- Mit Linux/Unix und Windows laufende Mailserver, darin eingeschlossen die von Sun Solaris Version 9 und höher erstellten Syslog-Meldungen zu „Auditing Services“.

Automatisieren der Verwaltung von DNS-Server-Ereignissen

Öffentliche DNS-Server werden häufig in der DMZ betrieben. GFI EventsManager kann die Ereignisse dieser Server automatisch erfassen und verarbeiten, darunter auch solche aus Protokollen von Windows-DNS-Servern.

Automatisieren der Verwaltung von Netzwerkgeräte-Ereignissen

Sehr häufig sind in einer DMZ auch Router und Firewalls zu finden. Beispielsweise schützen Router der Cisco IOS-Serie oder spezielle Firewalls das interne Netzwerk und stellen darüber hinaus besondere Funktionen wie die Port Address Translation (PAT) bereit, mit der sich die Systemleistung steigern lässt.

Wird GFI EventsManager in der DMZ installiert, können von dieser Hardware ausgegebene Ereignisse ebenfalls erfasst werden. Beispielsweise kann die GFI-Lösung als Syslog-Server fungieren und von Cisco IOS-Routern ausgegebene Nachrichten in Echtzeit erfassen.

Verwalten von Ereignissen von Microsoft Windows Vista und Windows Server 2008

Mit den Plattformen Microsoft Windows Vista und Windows Server 2008 wurden die Protokollierung von Ereignissen und die Verwaltung der Ereignisprotokolle im Hinblick auf die Strukturierung umfassend überarbeitet. Die wichtigsten Änderungen sind:

- Ein neues, auf XML basierendes Ereignisprotokoll-Format. Es erlaubt eine strukturiertere Darstellung sämtlicher System-ereignisse.
- Die neue Einteilung von Ereignissen in folgende unterschiedliche Typen: „Administrativ“, „Operationell“, „Audit“, „Analytisch“ und „Debug“
- Ein neues Dateiformat „evtx“, das das alte Ereignisarchiv-Format „evt“ ersetzt.

Hinweis 1: GFI EventsManager muss auf einem Vista-System installiert sein, um dessen Ereignisse erfassen und verarbeiten zu können.

Hinweis 2: GFI EventsManager muss auf einem Windows 2008-System installiert sein, um dessen Ereignisse erfassen und verarbeiten zu können.

Hardware-Anforderungen

Installationscomputer mit Microsoft Windows 2000/XP/2003

- Prozessor: CPU mit mindestens 2 GHz
- RAM: 512 MB
- Festplattenspeicher: mindestens 1,5 GB freier Festplattenspeicher
- Weitere Anforderungen: Tastatur und Maus oder kompatible Eingabe- und Zeigegeräte.

Installationscomputer mit Microsoft Windows Vista

Zur Verarbeitung von Ereignissen unter Microsoft Windows Vista muss GFI EventsManager auf einem Vista-Computer mit mindestens folgenden Anforderungen installiert und betrieben werden:

- Prozessor: CPU mit mindestens 2,8 GHz
- RAM: 2 GB
- Festplattenspeicher: mindestens 1,5 GB freier Festplattenspeicher
- Weitere Anforderungen: Tastatur und Maus oder kompatible Eingabe- und Zeigegeräte.

Software-Anforderungen

Installationscomputer

- Microsoft Windows 2000, XP, 2003, Vista
- Microsoft .NET Framework 2.0
- Microsoft Data Access Components (MDAC) 2.8 oder später
- Zugriff auf MSDE/SQL Server 2000 oder später

Zu überprüfende Computer

- Für Scans der Ereignisprotokolle von Microsoft Windows 2000, XP, 2003 und Vista:
    - Aktivierte Remote-Registrierung.
    - Aktivierte Überwachung von Sicherheitsereignissen unter Microsoft Windows.
    - Überwachte Vista-Computer müssen sich in derselben Domäne wie der GFI EventsManager-Computer befinden und die Benutzerkontosteuerung (User Account Control UAC) deaktiviert haben. Informationen zur Deaktivierung der UAC finden Sie hier: (in englischer Sprache) http://technet2.microsoft.com/WindowsVista/en/library/0d75f774-8514-4c9e-ac08-4c21f5c6c2d91033.mspx?mfr=true.
- Zur Kontrolle der W3C-Protokolle:
    - Quellverzeichnisse müssen über Windows-Freigaben zugänglich sein.
- Syslog-Meldungen und SNMP-Traps:
    - Quellen/Absender müssen für den Versand von Meldungen an den Computer/die IP-Adresse mit GFI EventsManager konfiguriert werden.

Aktualisieren einer früheren Version

Eine Aktualisierung von GFI EventsManager 7.0 oder 7.1 auf Version 8 erfolgt in wenigen Schritten. Nachfolgend erfahren Sie unter „Starten der Installation“, wie Sie das Update Installieren.

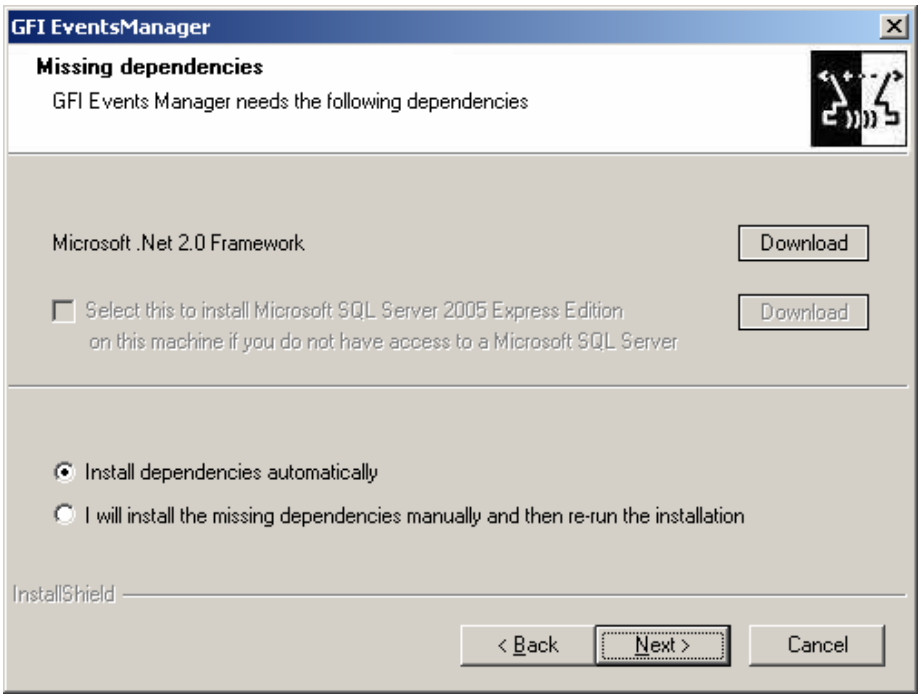
Aufgrund wesentlicher technologischer Änderungen ist eine Aktualisierung früherer Versionen als Version 7.0 von GFI EventsManager nicht möglich. Sie können jedoch eine solche ältere Version neben GFI EventsManager 8 als Vollprodukt parallel auf demselben Computer installieren, ohne dass ein Versionskonflikt auftritt.

Starten der Installation

Bei der Installation von GFI EventsManager werden Sie von einem Assistenten unterstützt. So starten Sie die Installation:

1. Schließen Sie alle geöffneten Anwendungen. Melden Sie sich über ein Benutzerkonto mit lokalen administrativen Zugriffsrechten am Computer an, auf dem das Produkt installiert werden soll.

2. Doppelklicken Sie auf die Installationsdatei **eventsmanager8.exe**.

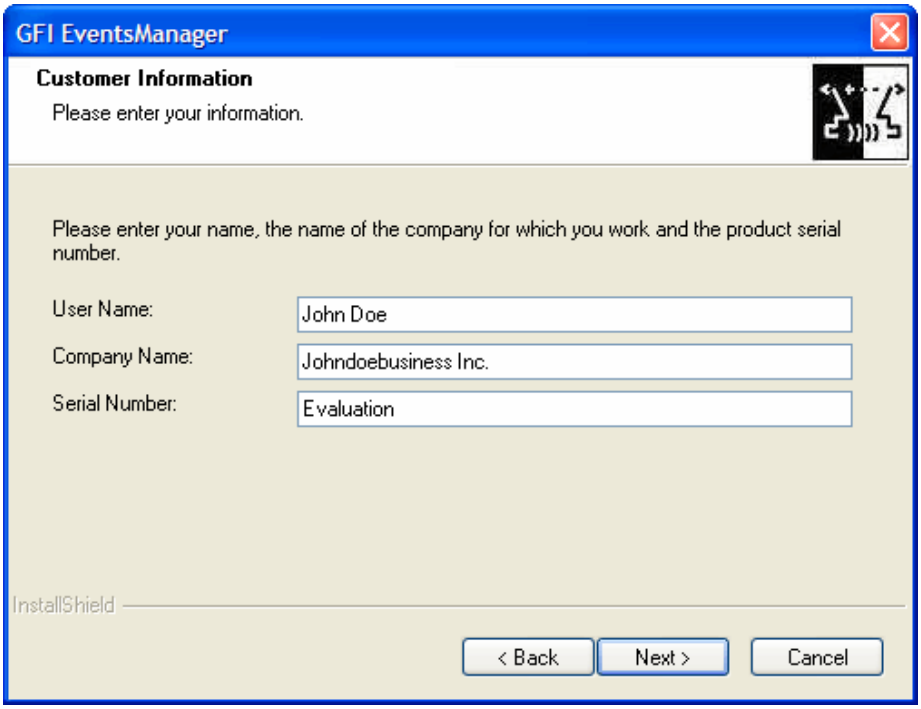

GFI EventsManager
Missing dependencies
GFI Events Manager needs the following dependencies
Microsoft .Net 2.0 Framework
Download
Select this to install Microsoft SQL Server 2005 Express Edition on this machine if you do not have access to a Microsoft SQL Server
Download
Install dependencies automatically
I will install the missing dependencies manually and then re-run the installation
InstallShield
< Back
Next >
Cancel

Screenshot 2 – Fehlende Abhängigkeiten

3. Fehlen grundlegende Abhängigkeiten, werden diese in einem gesonderten Dialogfenster angezeigt und können automatisch (durch Auswahl von **Install dependencies automatically**) oder manuell (durch Auswahl von **I will install the missing dependencies manually and then re-run the installation**) installiert werden.

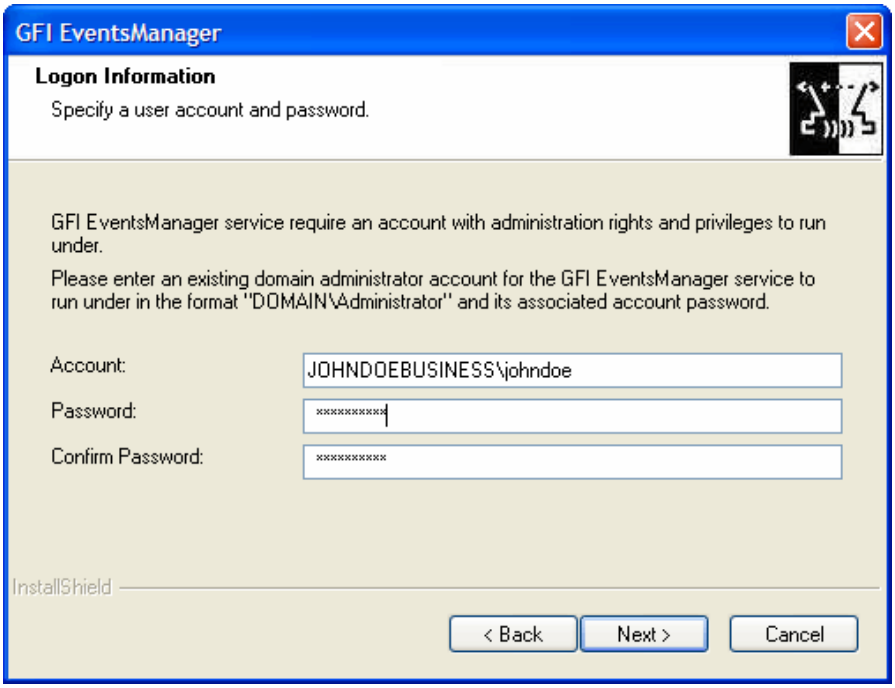
4. Klicken Sie im Willkommen-Bildschirm auf die Schaltfläche **Next**, um mit der Installation zu beginnen.

5. Lesen Sie die Lizenzvereinbarung. Wählen Sie die Option **I accept the licensing agreement** aus, damit die Installation fortgesetzt wird. Klicken Sie auf die Schaltfläche **Next**.



Screenshot 3 – Angaben zum Benutzer und Registrierschlüssel

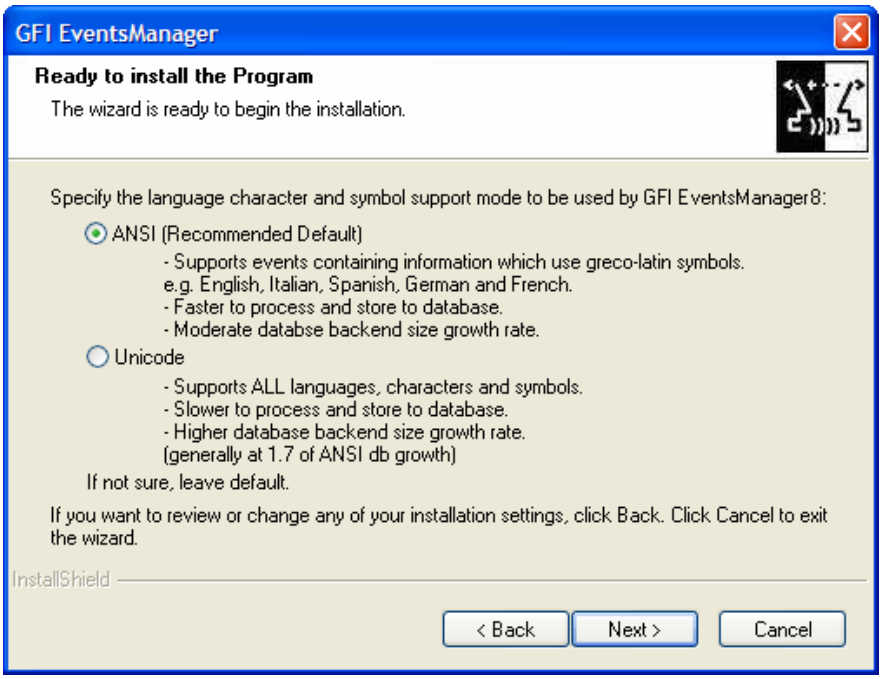
6. Geben Sie Ihren Namen, den Namen Ihres Unternehmens und den Registrierschlüssel ein. Wenn Sie das Produkt zu Testzwecken einsetzen, ändern Sie den vorgegebenen Eintrag „Evaluation“ bitte nicht. Klicken Sie auf die Schaltfläche **Next**.


GFI EventsManager
Logon Information
Specify a user account and password.
GFI EventsManager service require an account with administration rights and privileges to run under.
Please enter an existing domain administrator account for the GFI EventsManager service to run under in the format "DOMAIN\Administrator" and its associated account password.
Account:
JOHNDOEBUSINESS\johndoe
Password:
Confirm Password:
InstallShield
< Back
Next >
Cancel

Screenshot 4 – Angabe von Zugangsdaten

7. GFI EventsManager muss über ein Benutzerkonto mit administrativen Zugriffsrechten auf die Domäne ausgeführt werden. Geben Sie den Benutzernamen und das Passwort des Domänenadministrator-Kontos ein und klicken Sie auf die Schaltfläche **Next**.

8. Falls erforderlich, ändern Sie den vorgegebenen Installationspfad und klicken Sie auf die Schaltfläche **Next**.


GFI EventsManager
Ready to install the Program
The wizard is ready to begin the installation.
Specify the language character and symbol support mode to be used by GFI EventsManager8:
ANSI (Recommended Default)
- Supports events containing information which use greco-latin symbols.
e.g. English, Italian, Spanish, German and French.
- Faster to process and store to database.
- Moderate databse backend size growth rate.
Unicode
- Supports ALL languages, characters and symbols.
- Slower to process and store to database.
- Higher database backend size growth rate.
(generally at 1.7 of ANSI db growth)
If not sure, leave default.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Next >
Cancel

Screenshot 5- Auswahl des Modus für Zeichensatz und Sonderzeichen

9. Legen Sie fest, welchen Zeichensatz GFI EventsManager verwenden soll (**ANSI** oder **Unicode**) und klicken Sie auf die Schaltfläche **Next**. Klicken Sie auf die Schaltfläche **Install**, um mit der Installation zu beginnen.

10. Klicken Sie nach Abschluss des Installationsvorgangs auf die Schaltfläche **Finish**, um die Installation abzuschließen.

Erste Schritte

Einführung

Was ist ein Computerprotokoll?

Ein Computerprotokoll besteht aus einer Sammlung von Ereigniseinträgen, über die sich der Verlauf von Aktivitäten in einem Netzwerk oder auf einem Computersystem überprüfen lässt („Audit-Trail“). Computerprotokolle werden vielfach gezielt für forensische Sicherheitsanalysen archiviert, da mit ihrer Hilfe Abläufe detailliert nachvollzogen werden können. Als Format werden Binärdateien, wie bei Windows-Protokollen, oder Textdateien, wie bei Syslog- oder W3C-Protokollen, verwendet.

Was ist ein Ereignis?

Ein Ereignis ist ein Protokolleintrag mit Informationen zu einem Vorkommnis oder einer Zustandsveränderung in einem Computersystem oder Netzwerk. Mit aufgeführt sind Details zu Datum und Uhrzeit des Ereigniseintritts und eine kurze Beschreibung. Ereignisse werden zur vereinfachten Suche und digitalen Spurensuche oft in chronologischer Reihenfolge gespeichert.

Was sind Windows-Ereignisprotokolle?

Windows-Ereignisprotokolle enthalten systematische Einträge zu Ereignissen, die auf Rechnern oder Netzwerken mit Microsoft Windows-Betriebssystemen eingetreten sind. Systeme mit Windows 2000/XP/2003/Vista zeichnen Ereignisse in drei vorgegebenen Ereignisprotokollen auf:

- **Anwendungsprotokoll**
- **Sicherheitsprotokoll**
- **Systemprotokoll**

Computer mit besonderen Aufgaben im Netzwerk, beispielsweise Domänen-Controller und DNS-Server, protokollieren Ereignisse in zusätzlichen Standardprotokollen:

- **Verzeichnisdienst-Protokoll**
- **Dateireplikationsdienst-Protokoll**
- **DNS-Server-Protokoll**

Windows-Ereignisprotokolle informieren über folgende Arten von Ereignissen:

Fehler – Fehlerereignisse weisen darauf hin, dass ein bedeutendes Problem wie Daten- oder Funktionalitätsverlust aufgetreten ist. Beispielsweise wird ein beim Computerstart nicht aufgerufener Treiber oder Dienst als Fehler protokolliert.

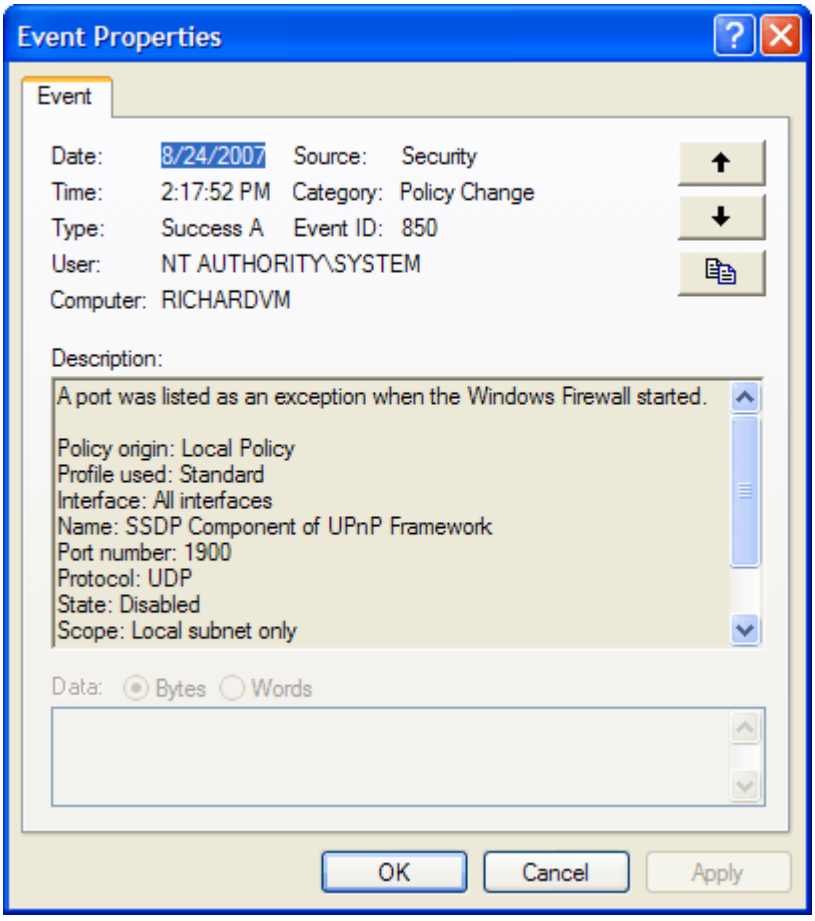
Warnung – Ein solches Ereignis muss keine akute Gefahr darstellen, könnte jedoch auf ein zukünftiges Problem hindeuten. Beispielsweise wird eine Warnung protokolliert, wenn der Festplattenspeicher zu Neige geht.

Information – Ein Ereignis, das den erfolgreichen Aufruf einer Anwendung, eines Treibers oder eines Diensts beschreibt. Beispielsweise wird beim erfolgreichen Laden eines Netzwerktreibers ein Ereignis der Kategorie „Information“ protokolliert.

Erfolgsüberwachung – Zeigt an, dass ein überwachtes Sicherheitsereignis erfolgreich abgeschlossen wurde. Beispielsweise wird bei einer erfolgreichen Anmeldung an einem Windows-Computer ein Erfolgsüberwachungs-Ereignis protokolliert.

Fehlversuchüberwachung – Zeigt an, dass ein überwachtes Sicherheitsereignis nicht erfolgreich abgeschlossen wurde. Ein Fehlversuch-Ereignis wird beispielsweise protokolliert, wenn einem Benutzer kein Zugriff auf ein Netzwerklaufwerk möglich war.

Der nachfolgende Screenshot zeigt einen gängigen Eintrag im Windows-Ereignisprotokoll.



Screenshot 6 – Windows-Ereignisprotokoll

Was sind W3C-Protokolle?

W3C-Protokolle kommen vorrangig bei Webservern zwecks Protokollierung Web-spezifischer Ereignisse zum Einsatz. Diese Protokolle werden unter Verwendung einer der beiden folgenden Formate in textbasierten Flat-Files geführt:

- W3C Common Log File Format
- W3C Extended Log File Format

Das W3C Common Log File Format wurde als Erstes veröffentlicht und hat als Standardformat vieler gängiger Webserver, darunter Apache, immer noch Bestand. Es besitzt jedoch den Nachteil, dass nur eine sehr eingeschränkte Auswahl an Daten zu Transaktionen des Servers protokolliert wird. Unberücksichtigt blieben beispielsweise wichtige Informationen zu Referrer, Agent, Übertragungszeit, Domänenname oder Cookies. Abhilfe schafft das neuere, im anpassbaren ASCII-Format vorliegende W3C Extended Log File Format, mit dem sich weitaus mehr Informationen erfassen lassen. Das W3C Extended Log File Format wird beispielsweise standardmäßig von den Microsoft Internet Information Services (IIS) verwendet.

Folgendes Beispiel zeigt einen gängigen Eintrag im W3C Extended Log File Format:

```
#Version: 1.0
#Date: 04-Sep-1996 00:00:00
#Fields: time cs-method cs-uri
00:34:23 GET /WebSRV/Pg_Snippet.html
12:21:16 GET /WebSRV/ Button_pg.html
12:45:52 GET /WebSRV/ Login_Pg.html
12:57:34 GET /WebSRV/ Error_msg.html
```

Was ist Syslog?

Syslog ist ein De-facto-Standard zur Protokollierung von Meldungen wie Systemereignissen in einem IP-Rechnernetz. Er dient üblicherweise der Aufzeichnung von Ereignissen auf Unix- oder Linux-Computern oder Netzwerkgeräten wie Cisco-Routern und Cisco PIX-Firewalls. Tritt ein Ereignis ein, wird dieses nicht direkt von einer Anwendung auf dem Gerät aufgezeichnet, sondern von diesem per kurze Textnachricht (Syslog-Meldung) an einen dedizierten Syslog-Server geschickt. Der Server sichert die Meldung in einer Protokolldatei. Syslog-Meldungen werden unverschlüsselt im Klartext verschickt; zur Verschlüsselung der Nachrichten kann jedoch ein SSL-Wrapper eingesetzt werden.

Syslog kommt häufig bei der Verwaltung von Computersystemen und Sicherheits-Audits zum Einsatz. Trotz einiger Schwachstellen hat es den Vorteil, von einer Vielzahl an Geräten unterstützt zu werden. Mithilfe des Syslog-Servers zur übergreifenden Erfassung lassen sich Protokolldaten vieler unterschiedlicher Systeme in einem zentralen Repository vereinen.

Für die Sicherung von Syslog-Meldungen/Ereignissen in Protokolldateien ist wiederum der Syslog-Daemon zuständig. Eine Syslog-Meldung besteht aus zwei Hauptkomponenten:

1. Der Kopfzeile („Header“) mit Datum/Uhrzeit und IP-Adresse oder Computername des Absendercomputers.

2. Die Meldung („Message“), bestehend aus Informationen zum Namen des zugehörigen Programms oder Untersystems und der eigentlichen Nachricht, getrennt durch einen Doppelpunkt.

Eine Syslog-Meldung kann wie folgt aussehen:

Sep 4 10:10:10 10.245.2.11 foo[421]: this is a message from WebSRV

Was sind SNMP-Traps?

SNMP-Traps helfen Netzwerk-Management-Systemen bei der Überwachung des Zustands von Elementen wie Routern, Firewalls oder Switches. Beispielsweise werden Informationen zur Betriebszeit von Geräten und zu Betriebssystemversionen kontrolliert sowie Interface-Daten erfasst. SNMP-fähige Hardware protokolliert Ereignisse nicht lokal, sondern sendet die Daten unaufgefordert zur Überprüfung direkt an einen SNMP-Trap-Server, der System-verantwortliche in wichtigen Fällen alarmiert.

GFI EventsManager bietet einen eigenen SNMP-Trap-Server, der SNMP-Meldungen empfängt, verarbeitet und bei Fehlfunktionen von Netzwerkelementen und anderen kritischen Ereignissen Administratoren informiert. Unterstützt werden Traps für die SNMP-Versionen 1, 2 und 3.

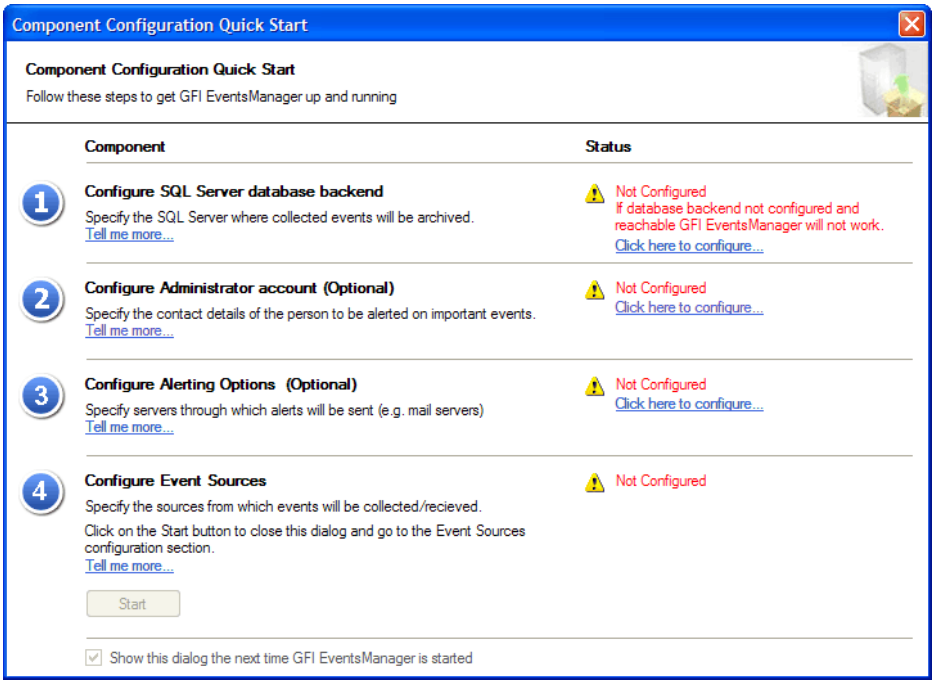
Was sind Überwachungsprotokolle von Microsoft SQL Server?

Microsoft SQL Server führt Ereignisprotokolle, die Administratoren beim Überwachen der Datenbankaktivität helfen. Die im Rahmen täglicher SQL-Server-Abläufe erstellten Protokolle zu Aktivitäten wie Server-Starts oder zu wichtigen Ereignissen wie fehlgeschlagenen Anmeldungen können mit GFI EventsManager verarbeitet werden. Werden bei der Überprüfung der Überwachungsprotokolle beispielsweise mehrere hintereinander fehlgeschlagene Anmeldeversuche festgestellt, kann eine Warnung erfolgen.

Erste Schritte: Starten von GFI EventsManager

Sämtliche Konfigurationseinstellungen zu GFI EventsManager erfolgen über die Verwaltungskonsole des Programms. So öffnen Sie die Verwaltungskonsole: Gehen Sie auf **Start ▸ Programme ▸ GFI EventsManager 8 ▸ Management Console**.

Erste-Schritte-Dialog


Component Configuration Quick Start
Component Configuration Quick Start
Follow these steps to get GFI EventsManager up and running
Component
Status
1
Configure SQL Server database backend
Specify the SQL Server where collected events will be archived.
Tell me more...
Not Configured
If database backend not configured and reachable GFI EventsManager will not work.
Click here to configure...
2
Configure Administrator account (Optional)
Specify the contact details of the person to be alerted on important events.
Tell me more...
Not Configured
Click here to configure...
3
Configure Alerting Options (Optional)
Specify servers through which alerts will be sent (e.g. mail servers)
Tell me more...
Not Configured
Click here to configure...
4
Configure Event Sources
Specify the sources from which events will be collected/recieved.
Click on the Start button to close this dialog and go to the Event Sources configuration section.
Tell me more...
Not Configured
Start
Show this dialog the next time GFI EventsManager is started

Screenshot 7 – Erste-Schritte-Dialog

Beim ersten Aufruf der Verwaltungskonsole nach der Produktinstallation wird der Schnellstart-Dialog zum Konfigurieren der einzelnen Komponenten von GFI EventsManager (**Component Configuration Quick Start**) geöffnet. Dieser unterstützt Sie bei der Festlegung der wichtigsten Parameter vor der Inbetriebnahme.

Folgende Parameter sind mit dem ersten Aufruf des Programms festzulegen:

Datenbank-Backend:

Geben Sie für die Ereignisarchivierung den Namen/die IP-Adresse des SQL-Servers und Informationen zum Datenbank-Backend an.

Daten des Administratorkontos von GFI EventsManager:

Geben Sie die E-Mail-Adresse und Mobilfunknummer des Administrators sowie den Namen/die IP-Adresse des Computers an, an den Warnungen geschickt werden.

Allgemeine Warnungen:

Legen Sie Daten des SMTP-Servers und SMS-Gateways/Service-Providers für E-Mail-/SMS-Warnungen fest.

Der Erste-Schritte-Dialog bietet Links zu den entsprechenden Konfigurationsmenüs, damit Sie alle erforderlichen Einstellungen schnell vornehmen können.

Konfigurieren des Datenbank-Backends

Über die Notwendigkeit der Protokollarchivierung

Für alle Umgebungen, in denen es auf die Einhaltung von Gesetzen (wie Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA)) und anderen Richtlinien zum Schutz und zur revisionssicheren Aufbewahrung von Daten ankommt, ist die Ereignisarchivierung von großer Bedeutung. Unternehmen sind verpflichtet, zentrale und geschützte Archive mit im Ursprungszustand belassenen Protokolldaten anzulegen. Diese müssen von den zur Echtzeit-Analyse verwendeten Daten getrennt sein.

GFI EventsManager erlaubt es Ihnen, sowohl verarbeitete als auch unverarbeitete Ereignisse per Microsoft SQL Server Datenbank-Backend zu archivieren. Neben der leichteren Einhaltung gesetzlicher Vorschriften bestehen dadurch folgende Vorteile:

- Ereignisse lassen sich zur detaillierten Analyse von Aktivitäten und zur Berichterstellung heranziehen.
- Es besteht ein einfacher Zugriff auf nach verschiedenen Kriterien gefilterte Ereignisse (bei verarbeiteten Protokollen)
- Unveränderte Protokolldaten liegen im Notfall als Backup vor.

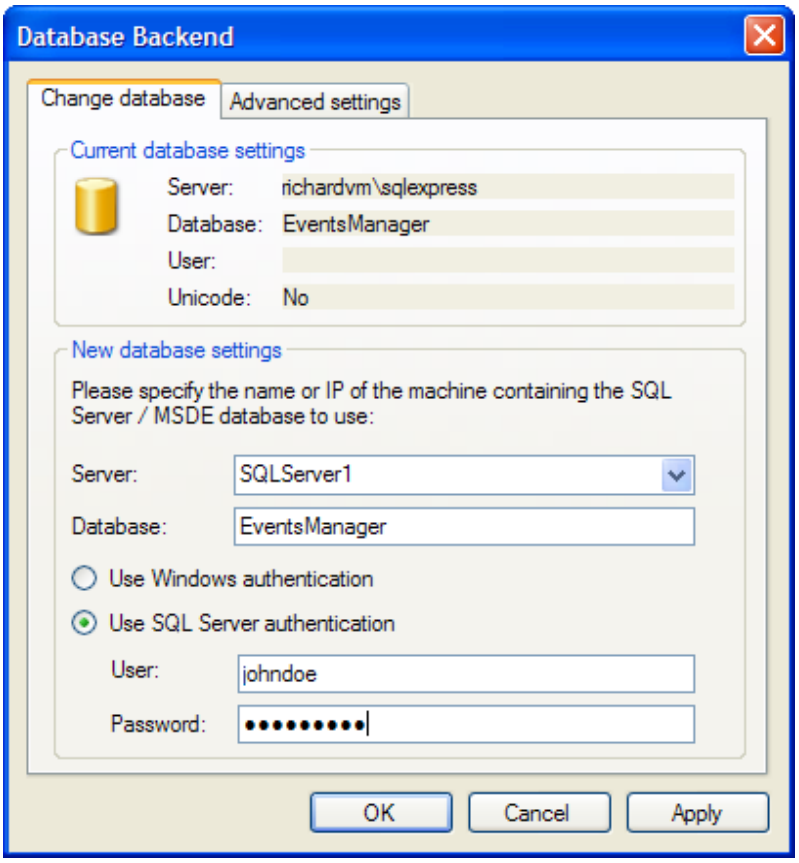
Zudem ist eine automatische Sicherung des Datenbank-Backends möglich. Hierbei kann eine Kopie der ursprünglichen Protokolldaten getrennt von den Daten zur Echtzeit-Analyse gesichert werden. Backups des Datenbank-Backends sind auch manuell durchführbar. Weitere Informationen hierzu erhalten Sie im Kapitel „Protokoll-Browser“ unter „Sichern von Ereignissen“.

Component
Status
Configure SQL Server database backend
Specify the SQL Server where collected events will be archived.
Tell me more...
Not Configured
If database backend not configured and recheable GFI EventsManager will not work.
Click here to configure...

Screenshot 8 – Erste-Schritte-Dialog: Link zum Konfigurieren des Datenbank-Backends

Um das Datenbank-Backend für die erste Verwendung zu konfigurieren, klicken Sie auf den entsprechenden Link im Erste-Schritte-Dialog.

Konfigurieren der SQL Server-Einstellungen



Screenshot 9 – Datenbank-Optionen, Reiter zur Änderung der Datenbank

So legen Sie die Einstellungen des SQL-Servers und Datenbank-Backends fest:

1. Geben Sie den Namen/die IP-Adresse Ihres SQL-Servers an.

2. Geben Sie den Namen des Datenbank-Backends an (z. B. EventsManagerDB).

3. Wählen Sie die für den SQL-Server erforderliche Authentifizierungsmethode aus. Bei Auswahl der SQL-Authentifizierung muss ein Benutzername und Passwort angegeben werden.

4. Klicken Sie auf den Reiter **Advanced settings**, um Einstellungen zum Zeichensatz und zu Sonderzeichen festzulegen.

5. Schließen Sie die Einrichtung der Konfigurationseinstellungen ab, indem Sie auf die Schaltfläche **OK** klicken.

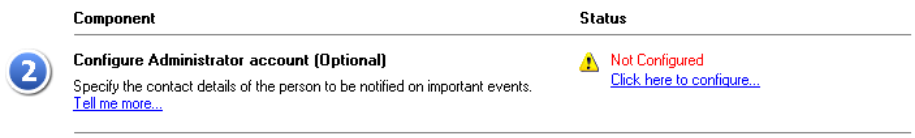
Konfigurieren des Administratorkontos von GFI EventsManager

Werden ausgewählte Ereignisse festgestellt, schickt GFI EventsManager automatisch eine Warnung per E-Mail, Netzwerknachricht oder SMS an festgelegte Empfänger. Zum korrekten Versand von Warnungen müssen für alle Empfänger die jeweils erforderlichen Kontaktinformationen angegeben werden.

Um die Durchführung von Verwaltungsaufgaben zu beschleunigen, lassen sich mehrere benutzerdefinierte Empfänger auch in Gruppen einteilen. Das Konto „EventsManagerAdministrator“ wird von GFI EventsManager automatisch eingerichtet. Sie müssen es jedoch mit Administratordaten konfigurieren. Hierfür reicht die Angabe der E-Mail-Adresse.

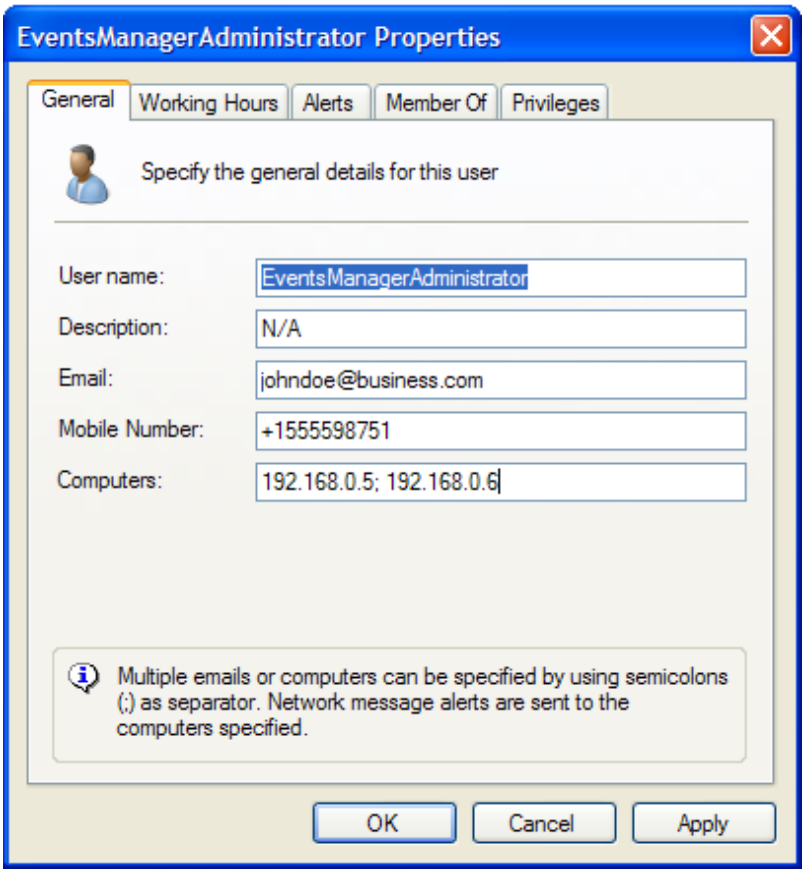
Folgende Einstellungen sind definierbar:

- Kontaktdaten wie E-Mail-Adresse und Telefonnummer
- Normale Geschäftszeiten (Kernarbeitszeit)
- Art der während und außerhalb der Geschäftszeiten zu verschickenden Warnung
- Benachrichtigungsgruppe, zu der der Benutzer gehört


Component
Status
Configure Administrator account (Optional)
Specify the contact details of the person to be notified on important events.
Tell me more...
Not Configured
Click here to configure...

Screenshot 10 – Erste-Schritte-Dialog: Link zur Konfigurierung des Administratorkontos

Um das Konto „EventsManagerAdministrator“ für die erste Verwendung zu konfigurieren, klicken Sie auf den entsprechenden Link im Erste-Schritte-Dialog.



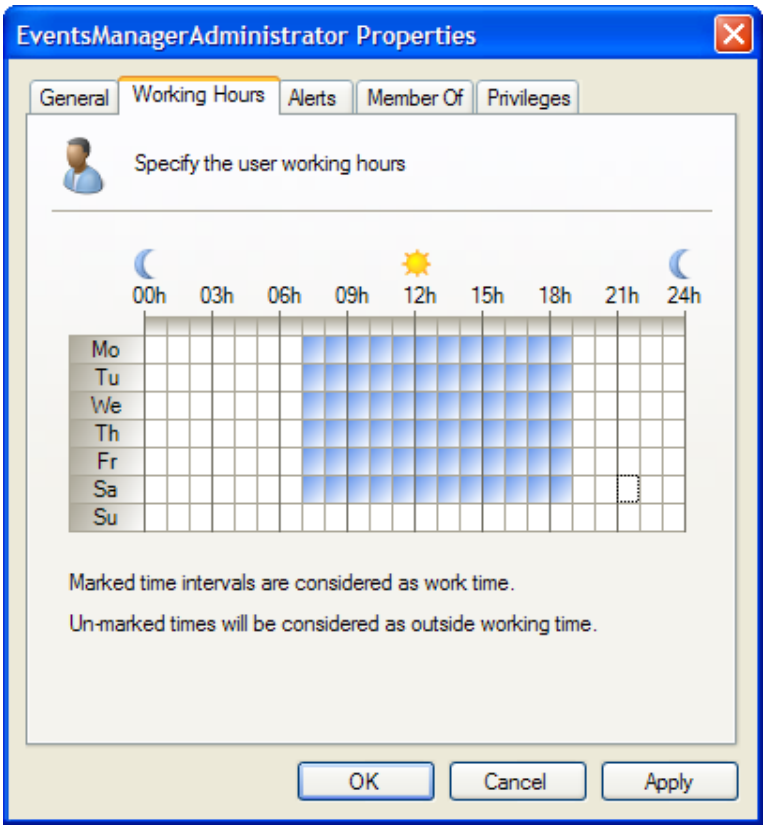
Screenshot 11 – Daten des GFI EventsManager-Administrators

Der Eigenschaften-Dialog für das Administratorkonto wird geöffnet. So legen Sie die Kontoeinstellungen fest:

1. Geben Sie die Kontaktdaten an (E-Mail-Adresse und ggf. Mobilfunknummer).

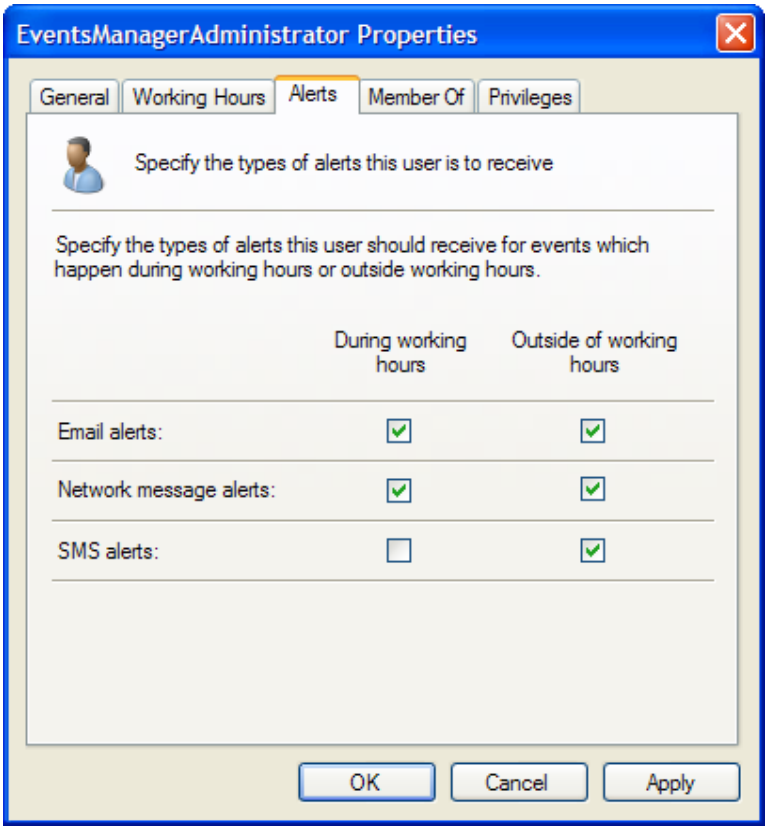
2. Geben Sie alle Computer an, an die für den Administrator bestimmte Warnungen per Netzwerknachricht geschickt werden sollen.

3. Klicken Sie auf den Reiter **Working Hours**.



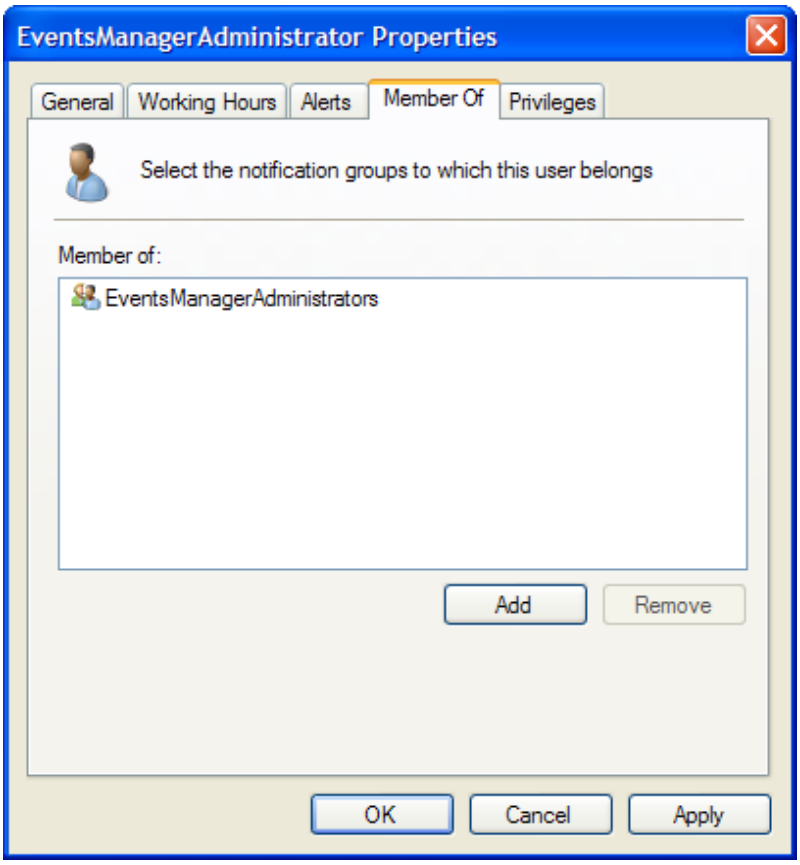
Screenshot 12 – Festlegen der typischen Arbeitszeit eines Warnungsempfängers

4. Geben Sie die typische Arbeitszeit des Administrators/Benutzers an.



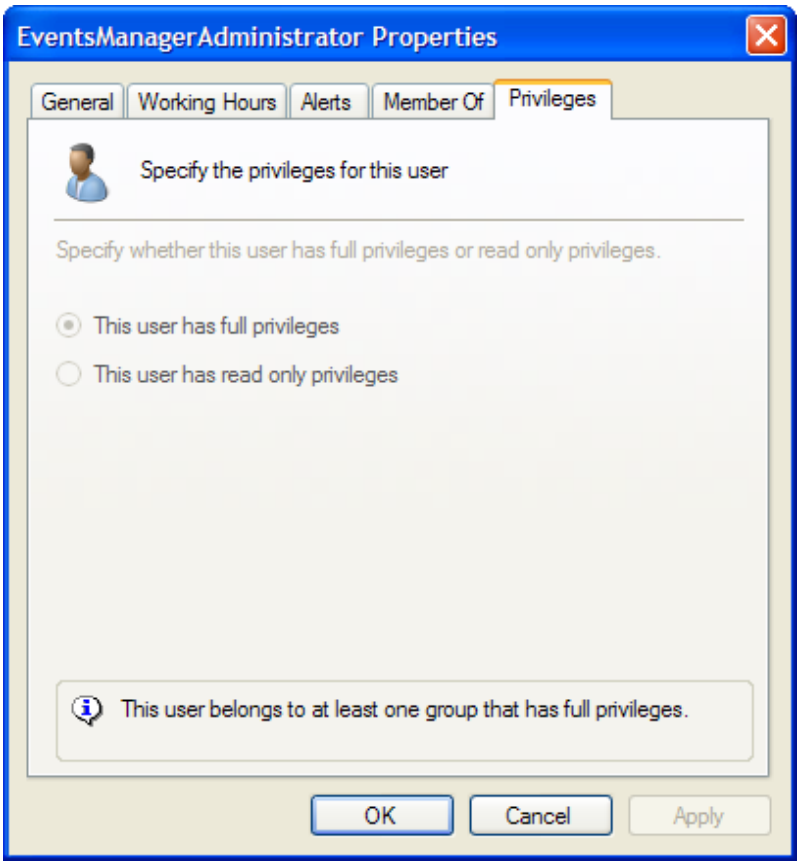
Screenshot 13 – Auswahl des Warnungstyps während/außerhalb der Arbeitszeit

5. Klicken Sie auf den Reiter **Alerts** und wählen Sie die Art der Warnung aus, die während und außerhalb der typischen Arbeitszeit des Administrators verschickt werden soll.



Screenshot 14 – Zugehörigkeit eines Benutzers zu einer Benachrichtigungsgruppe

6. Klicken Sie auf den Reiter **Mitglied von** und wählen Sie die Benachrichtigungsgruppe aus, zu der der Benutzer gehört. Administratoren sind standardmäßig Mitglied der Benachrichtigungsgruppe „EventsManagerAdministrator“.



Screenshot 15 – Einstellungen der Administrator-Zugriffsrechte

7. Klicken Sie auf den Reiter **Privileges** und wählen Sie die Option **This user has full privileges**, um dem Administrator Vollzugriffsrechte zuzuweisen.

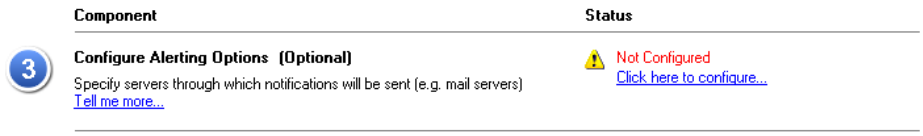
Hinweis: Benutzer mit Vollzugriffsrechten können sämtliche Konfigurationseinstellungen von GFI EventsManager bearbeiten.

8. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen fertig zu stellen.

Änderungen an den Eigenschaften des Administratorkontos können später jederzeit vorgenommen werden. Weitere Informationen hierzu erhalten Sie im Kapitel „Konfigurieren von Benutzern und Gruppen“.

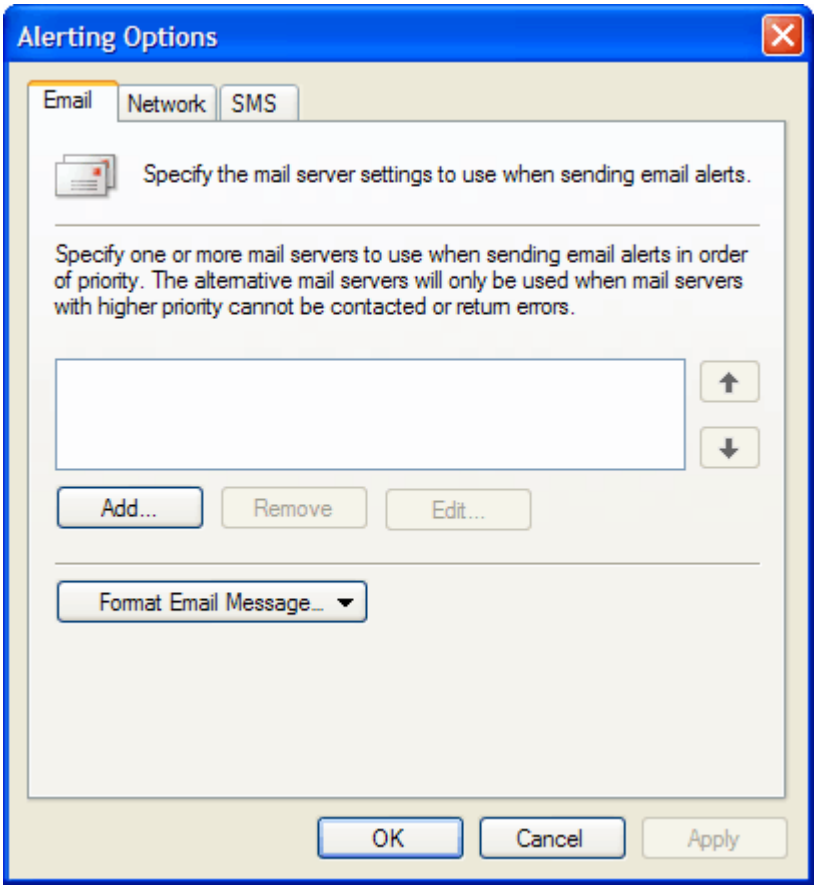
Konfigurieren allgemeiner Optionen für Warnungen

Werden (sicherheits)relevante Ereignisse festgestellt, verschickt GFI EventsManager automatisch eine Warnung per E-Mail, Netzwerknachricht oder SMS. Für den Versand der einzelnen Arten von Warnungen müssen auf das Netzwerk abgestimmte Parameter festgelegt werden. Beispielsweise ist für den Versand von E-Mail-Warnungen ein SMTP-Server anzugeben.



Screenshot 16 – Erste-Schritte-Dialog: Link zu Standardoptionen für Warnungen

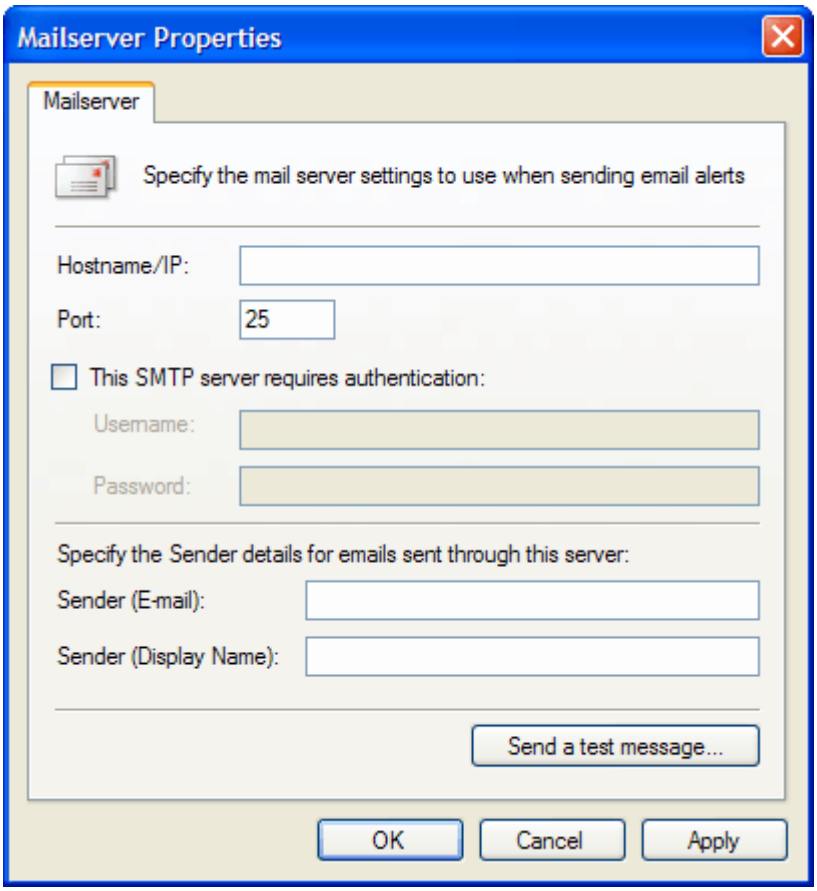
Um die allgemeinen Warnungsparameter erstmalig zu konfigurieren, klicken Sie im Erste-Schritte-Dialog auf den Link **Configure Alerting Options**.


Alerting Options
Email
Network
SMS
Specify the mail server settings to use when sending email alerts.
Specify one or more mail servers to use when sending email alerts in order of priority. The alternative mail servers will only be used when mail servers with higher priority cannot be contacted or return errors.
Add...
Remove
Edit...
Format Email Message...
OK
Cancel
Apply

Screenshot 17 – Optionen für den Versand von Warnungen

Das Dialogfeld **Alerting Options** wird geöffnet. Die Standard-einstellungen für Warnungen per E-Mail, Netzwerknachricht und SMS sind über die jeweiligen Reiter dieses Dialogs festzulegen. Weitere Informationen zur Konfigurierung dieser Einstellungen erhalten Sie nachfolgend.

Konfigurieren von E-Mail-Warnungen



Screenshot 18 – Eigenschaften des Mailservers

So legen Sie die Einstellungen für E-Mail-Warnungen fest:

1. Klicken Sie unter dem standardmäßig geöffneten Reiter **Email** auf die Schaltfläche **Add**, um die neuen Parameter anzugeben.

2. Geben Sie den Namen/die IP-Adresse Ihres Mailservers an. Sofern erforderlich, geben Sie zudem die Authentifizierungsdaten an.

3. Geben Sie die E-Mail-Adresse und den Anzeigenamen des Absenders von E-Mail-Warnungen an.

4. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen fertig zu stellen.

5. Klicken Sie auf die Schaltfläche **Format Email Message...**, falls Sie den per E-Mail verschickten Mitteilungstext überprüfen und anpassen möchten.

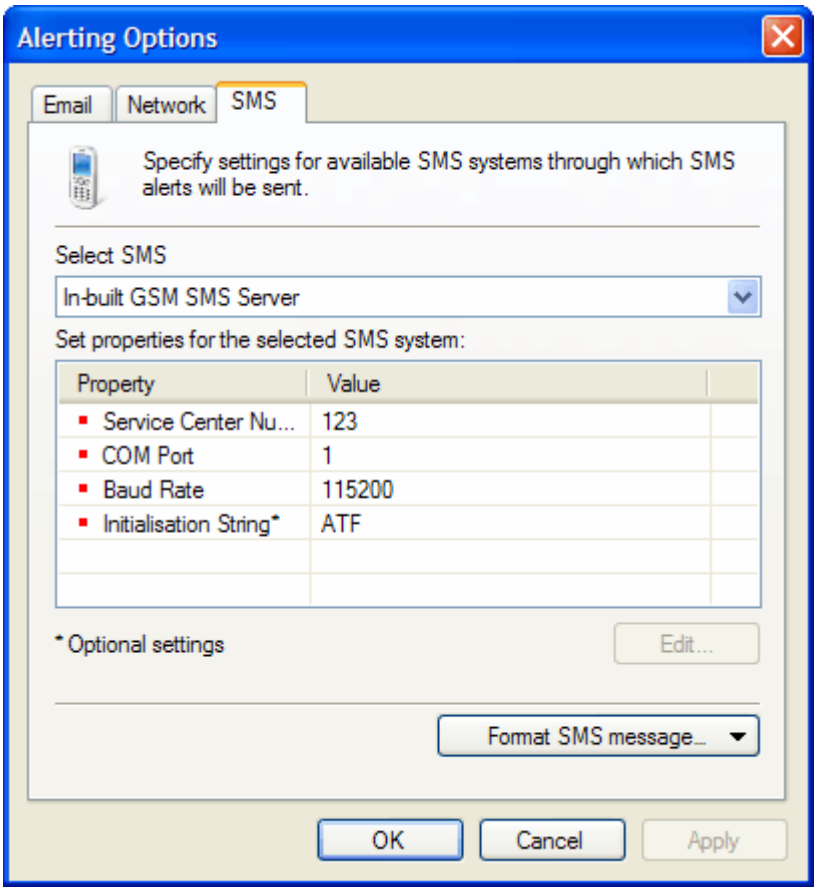
6. Sofern erforderlich, klicken Sie danach auf die Reiter **Network** oder **SMS**, um die jeweiligen Einstellungen vorzunehmen.

7. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen fertig zu stellen.

Konfigurieren von Warnungen per Netzwerknachricht

Für Warnungen per Netzwerknachricht sind über diesen Dialog keine gesonderten Einstellungen vorzunehmen. Der Inhalt der Mitteilung lässt sich jedoch per Klick auf die Schaltfläche **Format network message…** ändern.

Konfigurieren von SMS-Warnungen



Screenshot 19 – Optionen für den Versand von Warnungen – SMS-Einstellungen

Für den Versand von SMS-Warnungen stehen verschiedene Möglichkeiten bereit, zum einen der SMS-Gateway von GFI FAXmaker, zum anderen der E-Mail-zu-SMS-Gateway als Webservice von Clickatell. So legen Sie fest auf welche Art SMS-Warnungen verschickt werden sollen:

1. Wählen Sie aus der Drop-Down-Liste **Select SMS** die gewünschte Versandmethode für SMS-Warnungen aus.

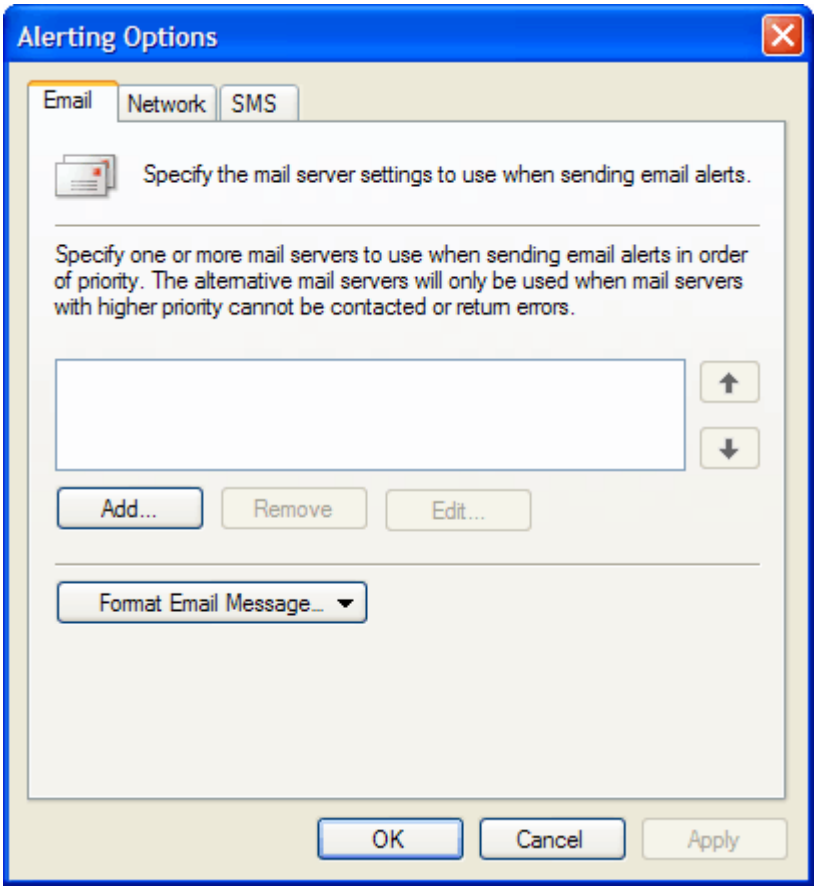
2. Wählen Sie aus der angezeigten Liste die zu ändernde Eigenschaft aus und klicken Sie auf die Schaltfläche **Edit**.

3. Führen Sie, falls erforderlich, Änderungen für die verbleibenden Einträge durch.

4. Der per SMS verschickte Inhalt der Mitteilung lässt sich per Klick auf die Schaltfläche **Format SMS message...** anpassen.

5. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen fertig zu stellen.

Ändern der allgemeinen Optionen für Warnungen


Alerting Options
Email
Network
SMS
Specify the mail server settings to use when sending email alerts.
Specify one or more mail servers to use when sending email alerts in order of priority. The alternative mail servers will only be used when mail servers with higher priority cannot be contacted or return errors.
Add...
Remove
Edit...
Format Email Message...
OK
Cancel
Apply

Screenshot 20 – Optionen für den Versand von Warnungen

Einstellungen der allgemeinen Optionen für den Versand von Warnungen können später jederzeit wie folgt geändert werden:

1. Klicken Sie in der Verwaltungskonsole auf den Reiter **Configuration**.

2. Klicken Sie auf die Ansicht **Options**.

3. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf den Knoten **Alerting Options** und wählen Sie im Kontextmenü **Edit alerting options**.

4. Konfigurieren Sie die Parameter wie oben beschrieben.

Erste Schritte: Verarbeiten von Ereignisprotokollen

Sämtliche zum ersten Start von GFI EventsManager erforderlichen grundlegenden Betriebsparameter sind jetzt definiert. Bevor Sie mit der eigentlichen Verarbeitung von Ereignisprotokollen beginnen können, sind Angaben erforderlich zu:

1. **Ereignisquellen**

   Der Name/die IP-Adresse der Computer, von denen Ereignisse zur Verarbeitung durch GFI EventsManager abgerufen werden.

2. **Zu verarbeitende Ereignisse**

   Alle Protokolle, die von GFI EventsManager verarbeitet werden sollen (Windows EVT, W3C, SNMP-Traps, Syslog, SQL-Server-Überwachungsprotokoll).

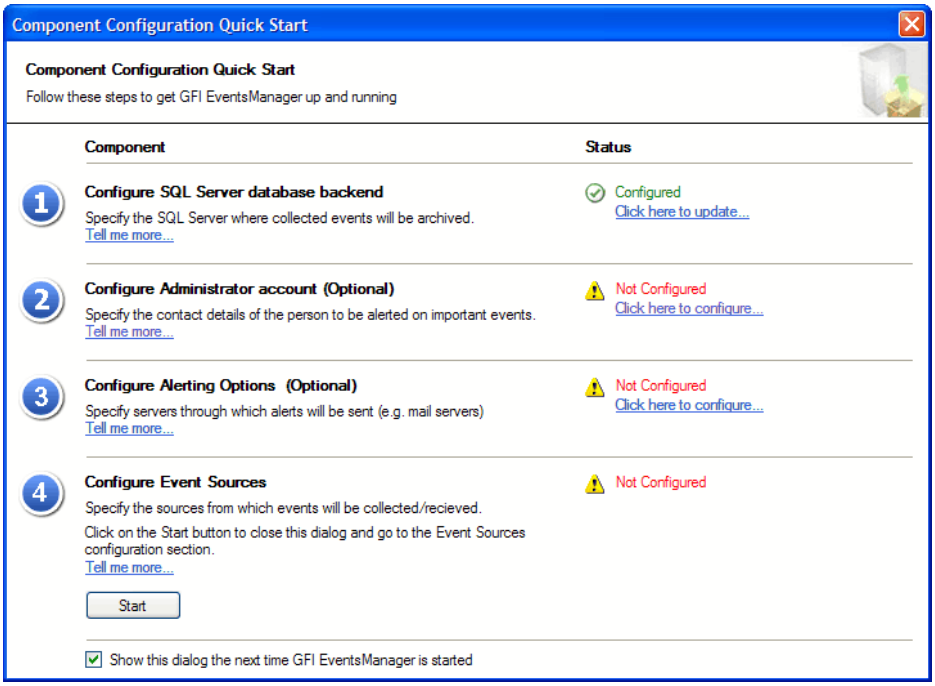
3. **Regeln zur Ereignisverarbeitung**

   Verarbeitungsregeln, die GFI EventsManager auf erfasste Protokolle anwenden soll.

4. **Warnungen und Aktionen**

   Warnungen und Aktionen, die aufgrund der Identifizierung bestimmter Ereignisse erfolgen sollen.

In den folgenden drei Kapiteln erhalten Sie Informationen zur Konfigurierung dieser Parameter.


Component Configuration Quick Start
Component Configuration Quick Start
Follow these steps to get GFI EventsManager up and running
Component
Status
Configure SQL Server database backend
Specify the SQL Server where collected events will be archived.
Tell me more...
Configured
Click here to update...
Configure Administrator account (Optional)
Specify the contact details of the person to be alerted on important events.
Tell me more...
Not Configured
Click here to configure...
Configure Alerting Options (Optional)
Specify servers through which alerts will be sent (e.g. mail servers)
Tell me more...
Not Configured
Click here to configure...
Configure Event Sources
Specify the sources from which events will be collected/recieved.
Click on the Start button to close this dialog and go to the Event Sources configuration section.
Tell me more...
Not Configured
Start
Show this dialog the next time GFI EventsManager is started

Screenshot 21 – Erste-Schritte-Dialog: Schaltfläche „Start“ zur Konfigurierung von Ereignisquellen

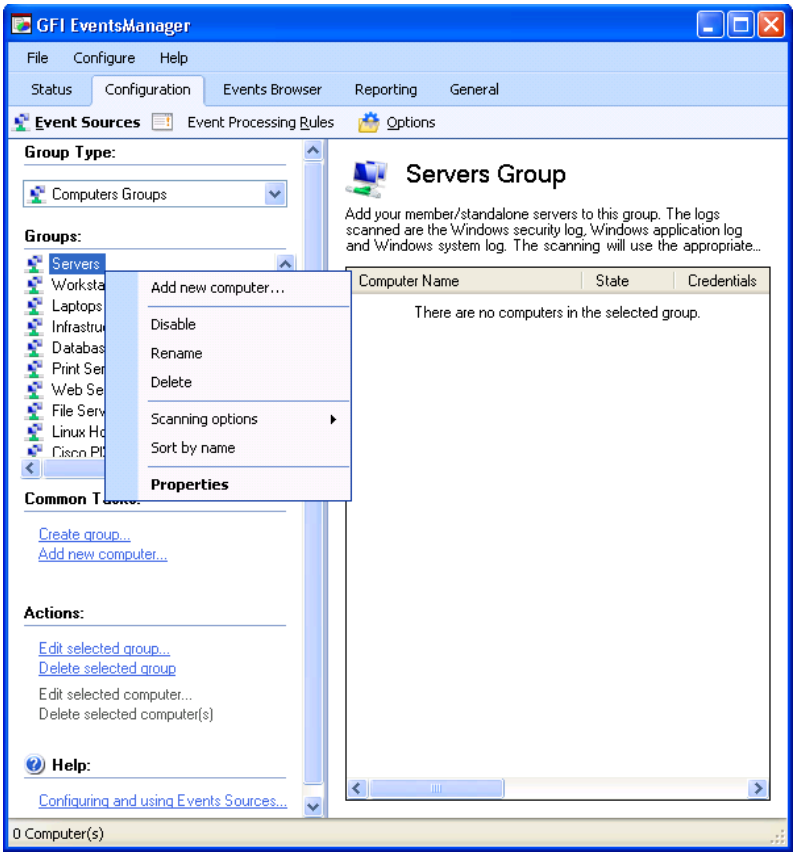
Klicken Sie unter Punkt 4 auf die Schaltfläche **Start**, um mit der Konfigurierung der Ereignisquellen fortzufahren. Weitere Informationen hierzu erhalten Sie im folgenden Kapitel „Konfigurieren von Ereignisquellen“.

Konfigurieren von Ereignisquellen

Einführung

Ereignisquellen sind Computer, auf denen sich von GFI EventsManager zu verarbeitende Protokolle befinden. Diese Quellen werden von GFI EventsManager in verschiedene Gruppen eingeteilt. Sie können an die Netzwerkinfrastruktur Ihres Unternehmens angepasste Gruppen erstellen oder bereits im Lieferumfang vorgegebene verwenden. In GFI EventsManager vordefiniert sind die beiden unterschiedlichen Gruppen **Computer Groups** und **Database Server Groups**. Standardmäßige Computergruppen können zur Verwaltung und Konfigurierung von zu überwachenden Servern, Workstations und Laptops genutzt werden. Ebenso lassen sich zu kontrollierende Zielrechner in einer Gruppe zusammenfassen, die in Ihrem Netzwerk eine besondere Funktion übernehmen, wie Webserver, Datei-Server und Daten-Server.

Hinzufügen neuer Ereignisquellen zu einer Gruppe der „Computers Groups“



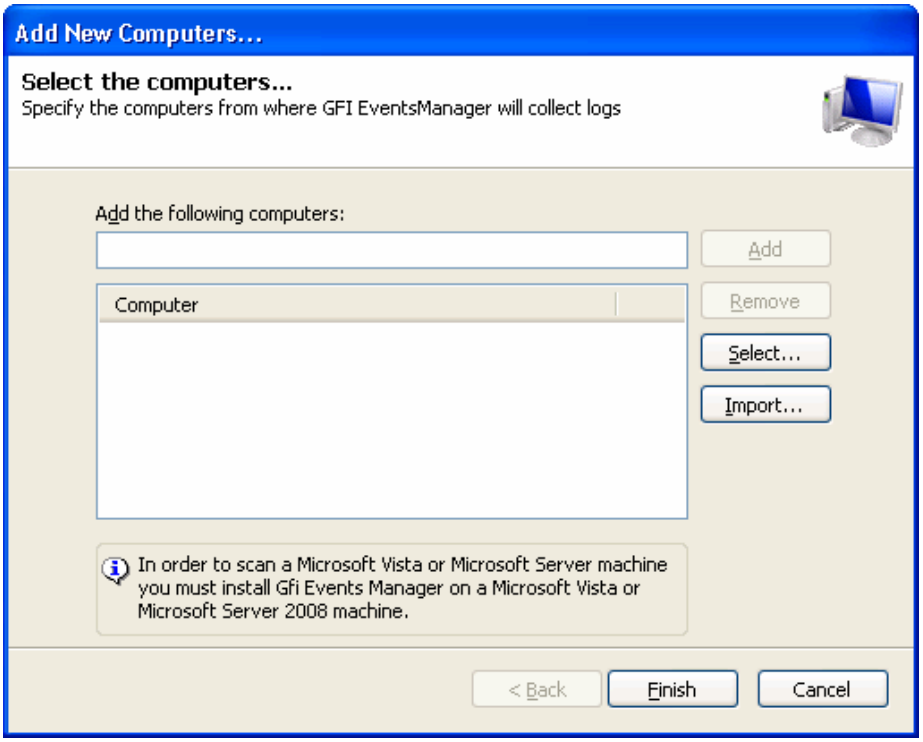
Screenshot 22 – Auswahl zu überwachender Computer

So erweitern Sie eine Computergruppe um neue Ereignisquellen:

1. Klicken Sie auf den Reiter **Configuration ▸ Event Sources**.

2. Wählen Sie aus der Drop-Down-Liste **Group Type** den Eintrag **Computers Groups** aus.

3. Klicken Sie im linken Fensterbereich im Bereich **Groups** mit der rechten Maustaste auf die Gruppe, der neue Ereignisquellen hinzugefügt werden sollen. Wählen Sie im Kontextmenü den Befehl **Add new computer**. Der Assistent zur Konfigurierung der neuen Computer wird aufgerufen.


Add New Computers...
Select the computers...
Specify the computers from where GFI EventsManager will collect logs
Add the following computers:
Add
Computer
Remove
Select...
Import...
In order to scan a Microsoft Vista or Microsoft Server machine you must install Gfi Events Manager on a Microsoft Vista or Microsoft Server 2008 machine.
< Back
Finish
Cancel

Screenshot 23 – Konfigurationsassistent: Festlegung neu zu überwachender Computer

4. Geben Sie den Namen/die IP-Adresse der neuen Ereignisquelle an. Klicken Sie auf die Schaltfläche **Add**, um die Quelle hinzuzufügen. Wiederholen Sie diesen Schritt, bis alle gewünschten Ereignisquellen der Gruppe hinzugefügt sind.

Hinweis: Klicken Sie auf die Schaltfläche **Import**, um eine Liste mit bereits in einer Textdatei definierten Ereignisquellen zu importieren. Klicken Sie auf die Schaltfläche **Select**, um Ereignisquellen aus einer Liste auszuwählen.

5. Klicken Sie abschließend auf die Schaltfläche **Fertig stellen**.

Hinweis: Nachdem Sie auf die Schaltfläche **Finish** geklickt haben, beginnt GFI EventsManager sofort mit dem Abruf von Protokollen der angegebenen Ereignisquellen.

Konfigurieren der Eigenschaften einer Ereignisquelle

Die Eigenschaften einer Ereignisquelle lassen sich an die betrieblichen Anforderungen Ihrer Infrastruktur anpassen. Parameter können festgelegt werden

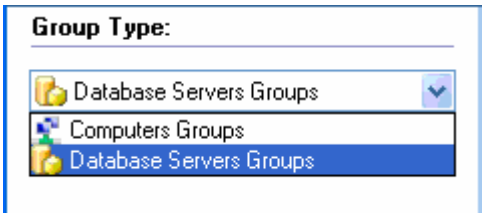
- je Computer
- je Computer-Gruppe

Folgende Eigenschaften einer Ereignisquelle können im Einzelnen angepasst werden:

- Allgemeine Eigenschaften wie der Name der Computergruppe
- Alternative Anmeldeinformationen des Domänenadministrators für den Remote-Zugriff auf die Ereignisprotokolle eines Zielrechners
- Üblicher Zeitraum für den Betrieb einer Ereignisquelle. Mit Hilfe dieser Parameter lassen sich relevante Ereignisse identifizieren, die außerhalb der normalen Betriebszeit eintreten, beispielsweise fehlgeschlagene Benutzeranmeldungen. In einem solchen Fall können Warnungen erstellt und zur sofortigen Kontrolle an Administratoren verschickt werden.
- Parameter zur Verarbeitung von Windows-, W3C- , SNMP- und Syslog-Ereignissen.

So konfigurieren Sie die Eigenschaften einer Ereignisquelle:

1. Klicken Sie in der Verwaltungskonsole auf den Reiter **Configuration**.



Screenshot 24 – Gruppentyp Datenbank-Server

2. Wählen Sie aus der Drop-Down-Liste **Group Type** den Eintrag **Computers Groups** aus.

3. So legen Sie die Einstellungen fest für

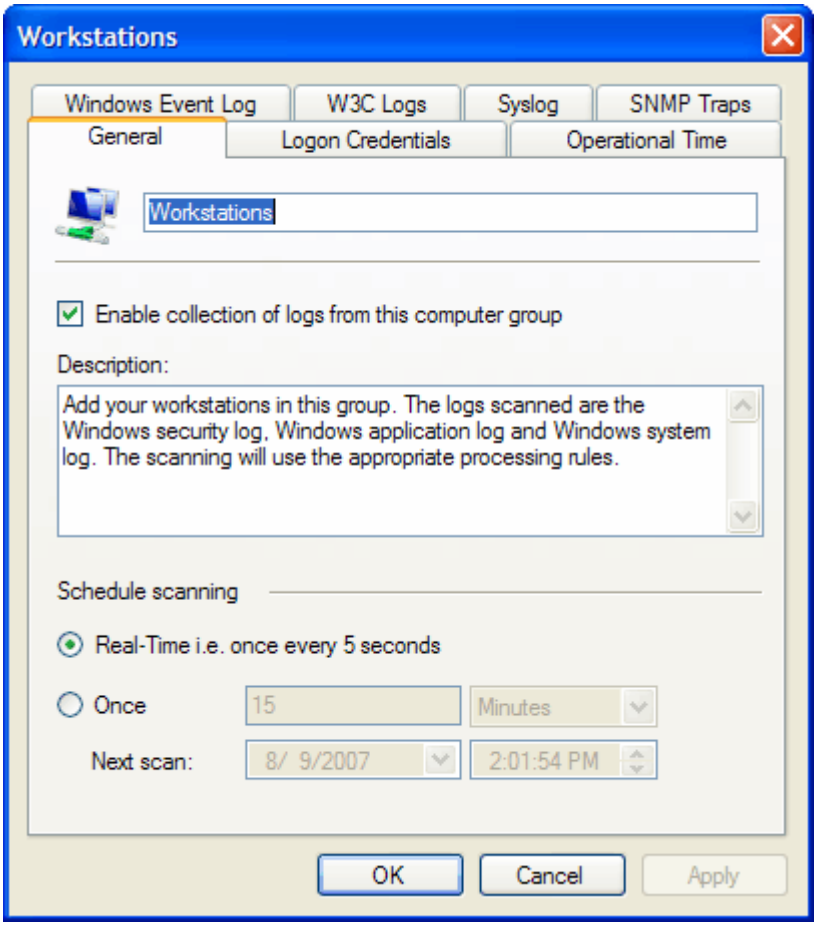
- eine Computer-Gruppe:
  Klicken Sie mit der rechten Maustaste auf die zu konfigurierende Computer-Gruppe und wählen Sie im Kontextmenü **Properties**.
- einen einzelnen Computer aus einer Computer-Gruppe:

  a) Klicken Sie auf die Gruppe, zu der der Computer gehört.

  b) Klicken Sie im rechten Fenster mit der rechten Maustaste auf den zu bearbeitenden Computer und wählen Sie im Kontextmenü **Properties**.

4. Klicken Sie auf die gewünschten Reiter, um die jeweiligen Einstellungen vorzunehmen. Weitere Informationen zu den einzelnen Reitern erhalten Sie nachfolgend.

Festlegen allgemeiner Eigenschaften einer Ereignisquelle



Screenshot 25 – Eigenschaften einer Computer-Gruppe

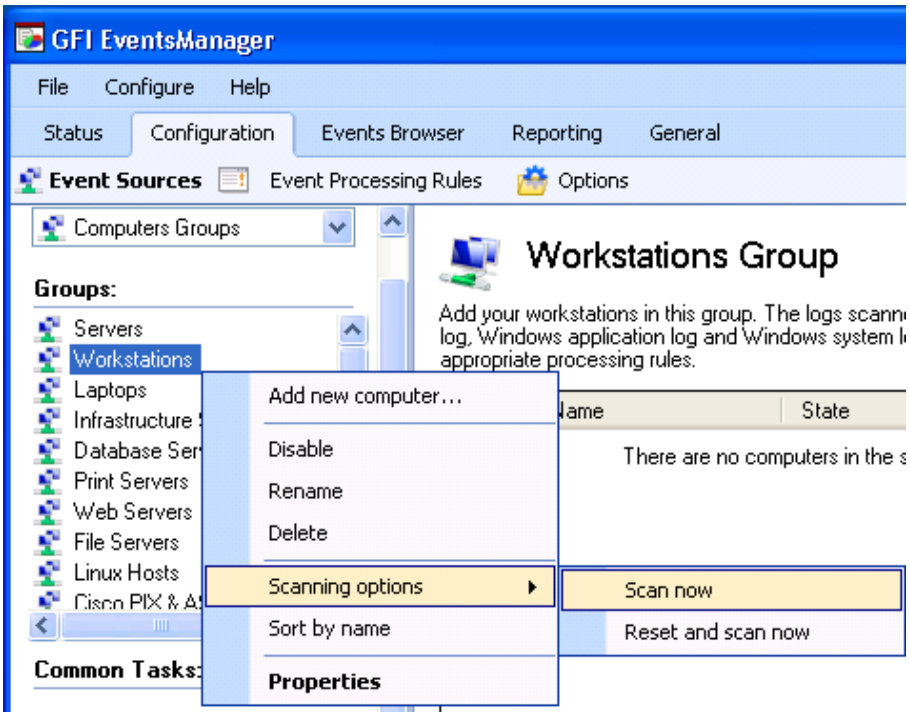
Folgende Einstellungen sind über den Reiter **General** möglich:

- Sie können den Namen einer Computer-Gruppe ändern.
- Sie können die Erfassung und Verarbeitung von Protokollen der Computer einer Gruppe aktivieren/deaktivieren.
- Sie können den Zeitplan für die Erfassung und Verarbeitung von Protokollen anpassen.

Festlegen alternativer Anmeldeinformationen des Domänenadministrators

Im Rahmen der Ereignisverarbeitung muss GFI EventsManager sich per Fernzugriff an den Zielcomputern anmelden. Die auf den Computer gespeicherten Protokolldaten werden abgerufen und an die Engine(s) zur Ereignisverarbeitung weitergeleitet.

Protokollerfassung und -verarbeitung sind ohne administrative Zugriffsrechte auf die Zielcomputer nicht möglich. GFI EventsManager meldet sich standardmäßig mit Hilfe der Anmeldeinformationen des Kontos, unter dem das GFI-Programm läuft, an den Zielcomputern an. Für einige Netzwerkumgebungen können jedoch eigene Zugangsdaten für den Administratorzugriff auf Workstations und Server erforderlich sein. So kann beispielsweise aus Sicherheitsgründen ein einzelnes, dediziertes Konto mit Zugriffsrechten allein auf Workstations und ein weiteres nur mit Rechten für Server vorhanden sein.



Screenshot 26 – Festlegen alternativer Anmeldeinformationen

GFI EventsManager erlaubt es Ihnen, gesonderte Anmeldeinformationen für einzelne Zielrechner wie auch für Computer-Gruppen zu definieren. So legen Sie Anmeldeinformationen für einzelne Computer/eine Computer-Gruppe fest:

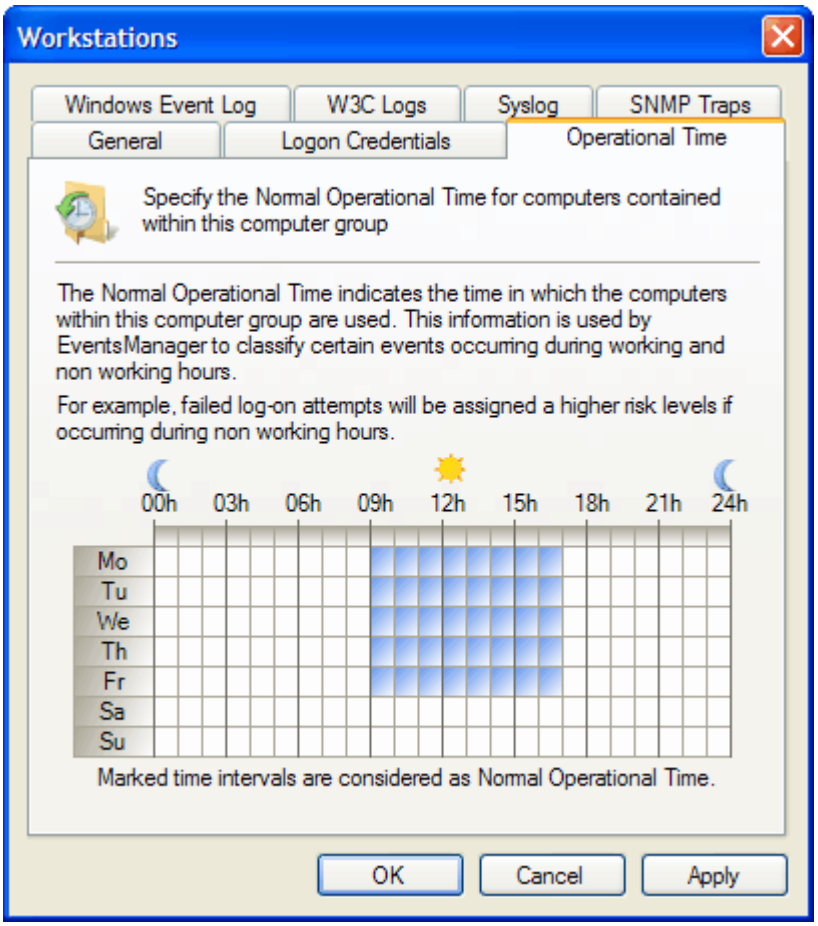
1. Öffnen Sie den jeweiligen Eigenschaften-Dialog wie zu Beginn dieses Kapitels beschrieben.

2. Klicken Sie auf den Reiter **Logon Credentials**.

3. Geben Sie den Benutzernamen und das Passwort an, das zur Anmeldung an den Zielrechnern und Erfassung der Protokolle erforderlich ist.

Konfigurieren der üblichen Betriebszeit einer Ereignisquelle

Mithilfe der Option **Operational Time** können Sie die übliche Betriebszeit angeben, in der die Ereignisquelle die meisten Aktivitäten verzeichnet (beispielsweise während der normalen Geschäftszeiten Ihres Unternehmens). Durch Angabe dieser Informationen kann GFI EventsManager zwischen Ereignissen unterscheiden, die innerhalb und außerhalb dieses Zeitraums liegen und sie entsprechend klassifizieren. Die so gewonnenen Daten erleichtern forensische Sicherheitsanalysen und das Aufspüren von Netzwerkrechnern, die außerhalb der normalen Geschäftszeiten entgegen Ihren Richtlinien verwendet wurden. Durch die zeitliche Festlegung können z. B. unbefugte Benutzerzugriffe, illegale Datentransfers und andere potenzielle Sicherheitsverletzungen im Netzwerk leichter festgestellt werden.

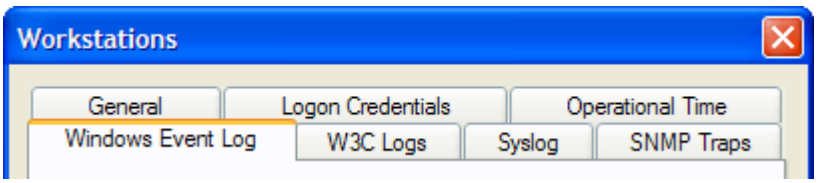


Screenshot 27 – Festlegung der üblichen Betriebszeit einer Ereignisquelle

Die Betriebszeit lässt sich für Computer-Gruppen festlegen. Über den Reiter **Operational Time** kann der Zeitraum der normalen Betriebszeit von in der Gruppe zusammengefassten Ereignisquellen in 1-Stunden-Schritten festgelegt werden.

Festlegen von Einstellungen für die Ereignisverarbeitung

So legen Sie die Einstellungen für die Ereignisverarbeitung fest:



Screenshot 28 – Reiter zur Konfigurierung der Ereignisverarbeitung (hier: Windows-Ereignisprotokoll)

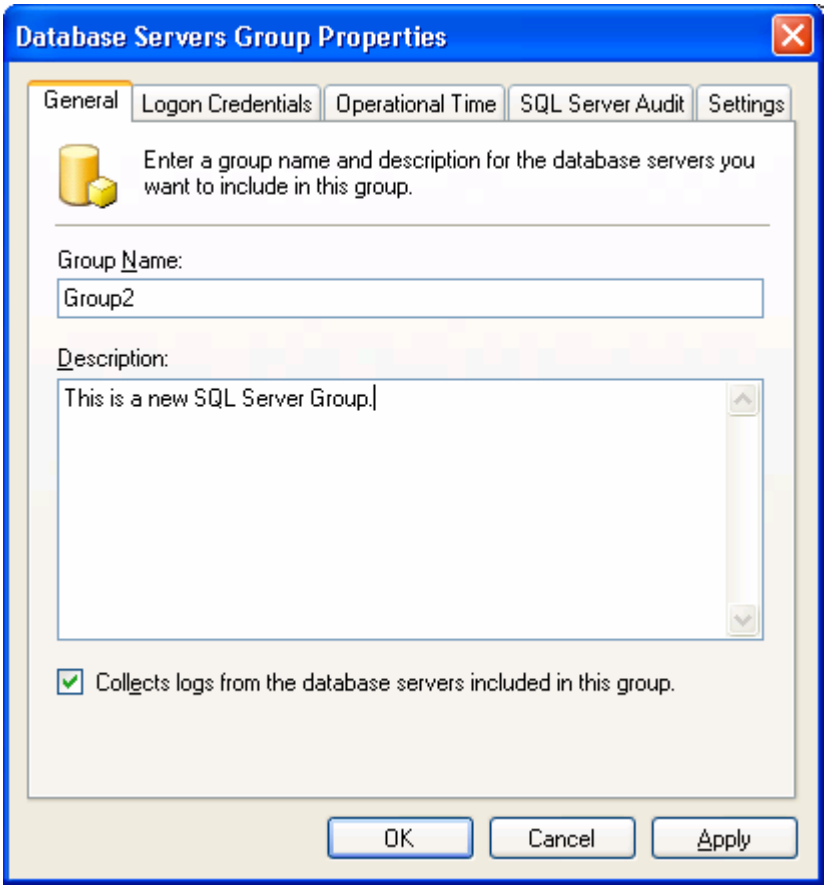
1. Öffnen Sie den jeweiligen Eigenschaften-Dialog wie zu Beginn dieses Kapitels beschrieben.

2. Gehen Sie auf den Reiter **Windows Event Log**, **W3C Logs**, **Syslog** und **SNMP Traps**, um die erforderlichen Einstellungen vorzunehmen. Detaillierte Hinweise zur Festlegung der einzelnen Parameter erhalten Sie im Kapitel „Konfigurieren von Regeln zur Ereignisverarbeitung“.

Hinzufügen einer neuen SQL-Server-Gruppe

1. Klicken Sie in der Verwaltungskonsole auf den Reiter **Configuration**.

2. Wählen Sie aus der Drop-Down-Liste **Group Type** den Eintrag **Database Servers Groups** aus.



Screenshot 29 – Erstellen einer neuen SQL-Server-Gruppe

3. Klicken Sie mit der rechten Maustaste auf eine bereits bestehende Gruppe und wählen Sie im Kontextmenü **Create group**, um eine neue Gruppe zu erstellen.

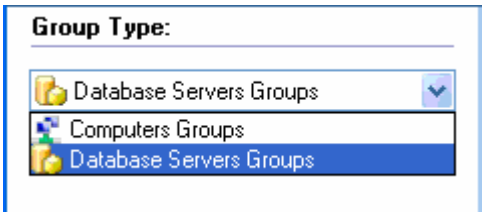
4. Legen Sie die Einstellungen der neuen SQL-Server-Gruppe fest. Weitere Informationen zu den einzelnen Reitern erhalten Sie in diesem Kapitel unter „Festlegen der Eigenschaften von SQL-Servern als Ereignisquelle“.

Festlegen der Eigenschaften von SQL-Servern als Ereignisquelle

Die Eigenschaften von SQL-Servern als Ereignisquelle können für eine gesamte Gruppe oder für einzelne SQL-Server festgelegt werden.

So legen Sie die Eigenschaften eines einzelnen SQL-Servers oder einer Gruppe aus SQL-Servern fest:

1. Klicken Sie in der Verwaltungskonsole auf den Reiter **Configuration**.



Screenshot 30 – Gruppentyp Datenbank-Server

2. Wählen Sie aus der Drop-Down-Liste **Group Type** den Eintrag **Database Servers Groups** aus.

3. So legen Sie die Einstellungen fest für

- eine Gruppe aus Datenbank-Servern: Klicken Sie mit der rechten Maustaste auf die zu konfigurierende Server-Gruppe und wählen Sie im Kontextmenü **Properties**.
- einen einzelnen Computer, der zu einer Gruppe aus Datenbank-Servern gehört: Klicken Sie in der Datenbank-Server-Gruppe auf die Gruppe, zu der der Computer gehört. Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf den zu bearbeitenden Computer und wählen Sie im Kontextmenü **Properties**.

4. Folgende Einstellungen können über die einzelnen Reiter festgelegt werden:

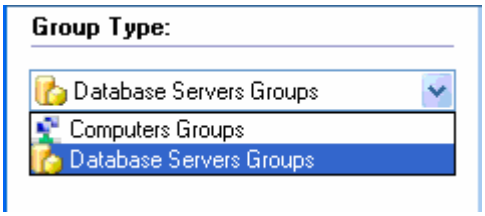
- **General –** Erlaubt es Ihnen, den Gruppennamen zu ändern.
- **Logon credentials –** Erlaubt es Ihnen, die Authentifizierungsmethode auszuwählen und ggf. Anmeldeinformationen anzugeben.
- **Operational time –** Ermöglicht es Ihnen, die übliche Betriebszeit der Datenbank-Server, die zur Gruppe gehören, anzugeben.
- **SQL-Server-Audit –** Ermöglicht es Ihnen festzulegen, welche Verarbeitungsregeln auf die erfassten Ereignisse angewendet werden sollen. Standardmäßig werden diese Einstellungen von der übergeordneten Datenbank-Server-Gruppe übernommen.
- **Settings –** Erlaubt es Ihnen, Optionen für Ereignis-Scans von SQL-Servern festzulegen, d. h. Scan aller Datenbanken, Scan einer festgelegten Datenbank oder alleiniger Scan von Sicherheitsereignissen für alle Datenbanken.

Erweitern der Standardgruppe um neue SQL-Server

Mit der Funktion zur Überwachung von SQL-Servern können die im Rahmen täglicher SQL-Server-Abläufe erstellten Protokolle zu Aktivitäten wie Server-Starts oder wichtigen Ereignissen wie fehlgeschlagenen Anmeldungen verarbeitet werden.

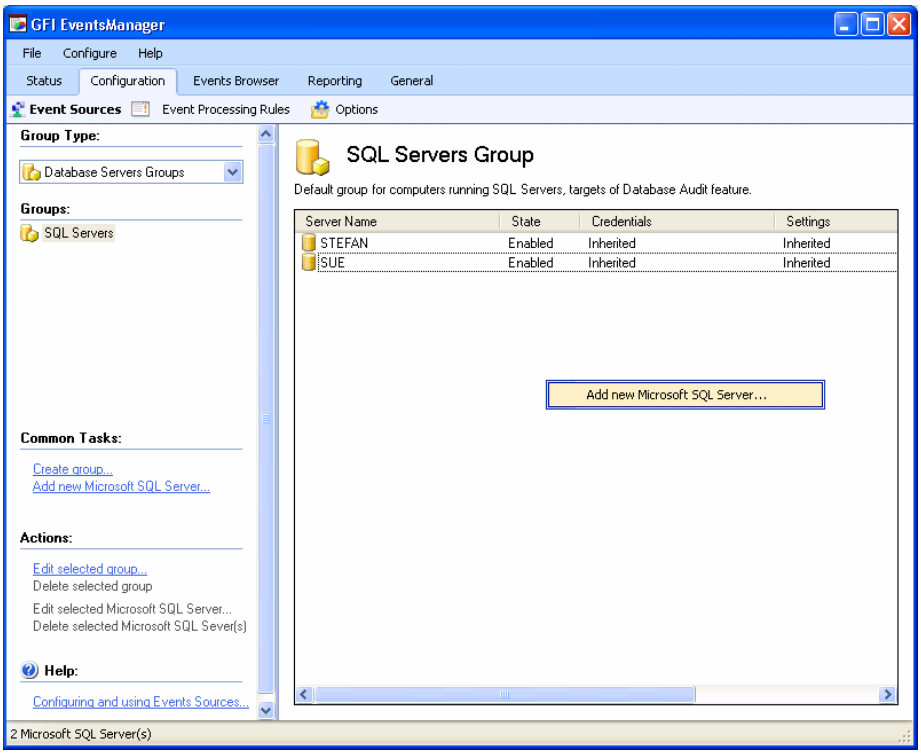
Ebenso wie normale Computer lassen sich auch SQL-Server in einer Gruppe organisieren und mit einer gemeinsamen Scan-Richtlinie für Ereignisprotokolle kontrollieren. So erweitern Sie eine SQL-Server-Gruppe:

1. Klicken Sie in der Verwaltungskonsole auf den Reiter **Configuration**.



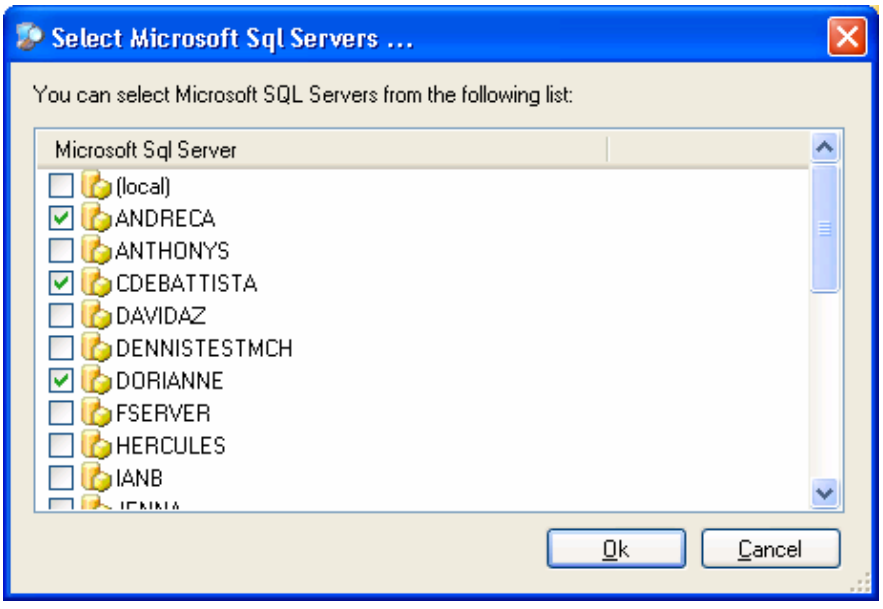
Screenshot 31 – Gruppentyp Datenbank-Server

2. Wählen Sie aus der Drop-Down-Liste **Group Type** den Eintrag **Database Servers Groups** aus.



Screenshot 32 – Hinzufügen eines neuen SQL-Servers

3. Klicken Sie an einer beliebigen Stelle im rechten Fenster auf die rechte Maustaste und wählen Sie im Kontextmenü **Add new Microsoft SQL Server**, um einen neuen SQL-Server hinzuzufügen.



Screenshot 33 – Auswahl aller hinzuzufügenden SQL-Server

4. Klicken Sie auf die Schaltfläche **Select** und wählen Sie alle gewünschten Server aus der angezeigten Liste aus. Klicken Sie auf die Schaltfläche **OK**.

5. Klicken Sie auf die Schaltfläche **Finish**, um die Einstellungen fertig zu stellen.

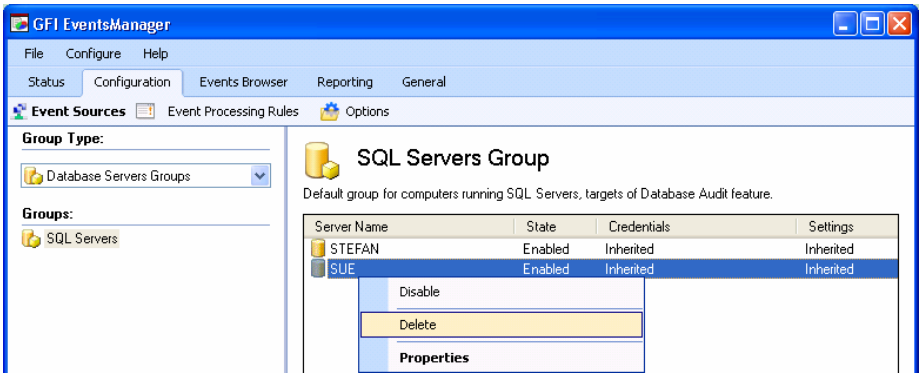
Hinweis: Der von GFI EventsManager aktuell als Datenbank-Backend verwendete SQL-Server kann nicht überwacht werden.

Entfernen von SQL-Servern aus der Standardgruppe

So entfernen Sie einen SQL-Server aus der Standardgruppe **Database Servers Group**:

1. Klicken Sie in der Verwaltungskonsole auf den Reiter **Configuration**.

2. Wählen Sie aus der Drop-Down-Liste **Group Type** den Eintrag **Database Servers Groups** aus.



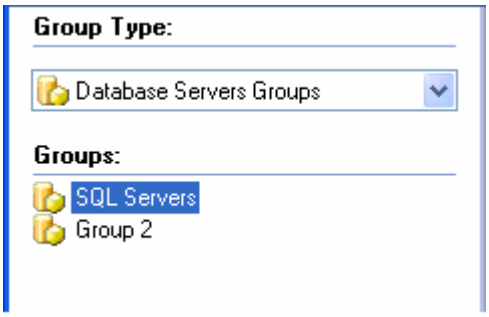
Screenshot 34 – Auswahl aller zu entfernenden SQL-Server

3. Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf den zu entfernenden SQL-Server und wählen Sie im Kontextmenü **Delete**.

Festlegen der Eigenschaften eines SQL-Servers

Standardmäßig übernimmt ein SQL-Server die Eigenschaften der übergeordneten Gruppe (im folgenden Beispiel: „SQL Servers“). So legen Sie die Eigenschaften eines SQL-Servers individuell fest:

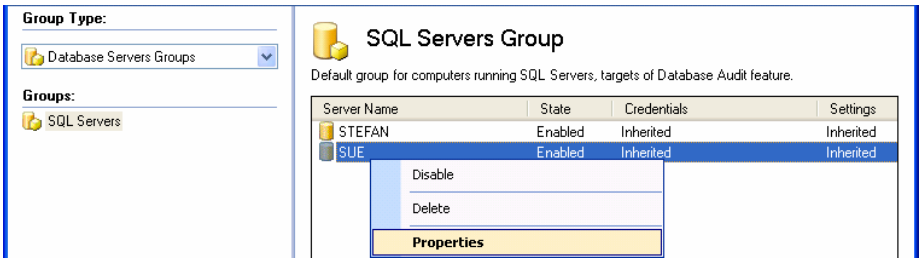
1. Klicken Sie in der Verwaltungskonsole auf den Reiter **Configuration**.



Screenshot 35 – Gruppe „SQL Servers“

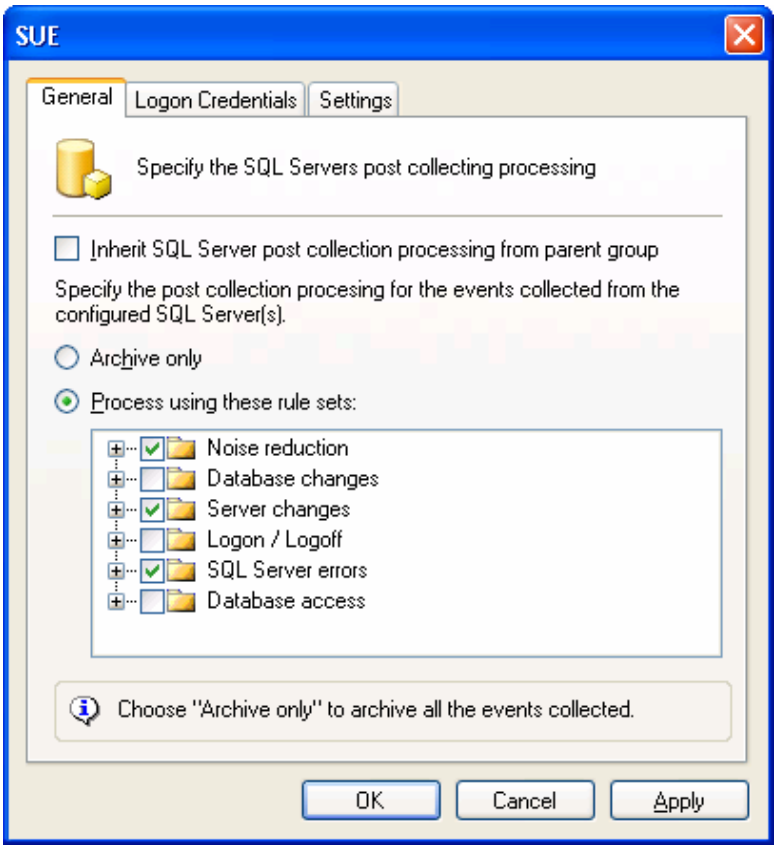
2. Wählen Sie aus der Drop-Down-Liste **Group Type** den Eintrag **Database Servers Groups** aus.

3. Wählen Sie im Bereich **Groups** die Gruppe mit dem zu bearbeitenden SQL-Server aus, im folgenden Beispiel „SQL Servers“.



Screenshot 36 – Eigenschaften eines SQL-Servers aus der Gruppe „SQL Servers“

3. Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf den SQL-Server, dessen Eigenschaften individuell festgelegt werden sollen, und wählen Sie im Kontextmenü **Properties**.



Screenshot 37 – Eigenschaften eines SQL-Servers

4. Folgende Einstellungen können über die jeweiligen Reiter vorgenommen werden:

- **General –** Ermöglicht es Ihnen, Verarbeitungsregeln festzulegen, die nach der Ereigniserfassung angewendet werden sollen. Standardmäßig werden die Einstellungen der übergeordneten Gruppe übernommen.
- **Logon credentials –** Erlaubt es Ihnen, die Authentifizierungsmethode auszuwählen und Anmeldeinformationen anzugeben, falls die SQL-Server-Authentifizierung gewählt wurde.
- **Settings –** Erlaubt es Ihnen, Optionen für Ereignis-Scans von SQL-Servern festzulegen, d. h. Scan aller Datenbanken, Scan einer festgelegten Datenbank oder alleiniger Scan von Sicherheitsereignissen für alle Datenbanken.

Erstellen von Regeln zur Ereignisverarbeitung

Einführung

GFI EventsManager unterstützt die Erfassung und Verarbeitung von Windows-Ereignisprotokollen, W3C-Protokollen, Syslog-Meldungen, SNMP-Traps und Microsoft SQL Server Überwachungsprotokollen. Die Protokolle führen Ereignisse in eigenen, proprietären Formaten, für die Einstellungen separat zu definieren sind. Einstellungen für die Protokollerfassung und -verarbeitung lassen sich konfigurieren:

- für jeden einzelnen Computer
- für jede einzelne Computer-Gruppe

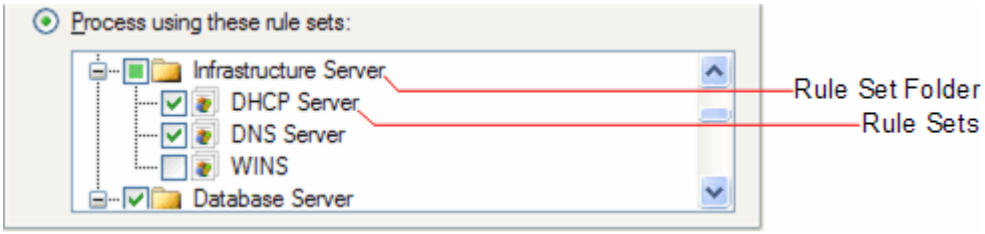
Bei der Verarbeitung von Ereignissen überprüft GFI EventsManager die erfassten Protokolle mit mehreren konfigurierbaren Regeln, auf deren Grundlage Ereignisse klassifiziert und gegebenenfalls Warnungen ausgegeben und Aktionen durchgeführt werden. Im Lieferumfang von GFI EventsManager sind bereits mehrere vordefinierte Regeln zur Ereignisverarbeitung enthalten, mit der sich Protokolle im gesamten Netzwerk ohne großen Konfigurations-aufwand erfassen und kontrollieren lassen.

Regeln zur Ereignisverarbeitung

Regeln zur Ereignisverarbeitung enthalten Anweisungen/Checks, die bewirken, dass

- erfasste Protokolle analysiert werden.
- Ereignisse klassifiziert werden: Die Einstufung erfolgt anhand der Einstellungen der jeweiligen Verarbeitungsregel.
- Ereignisse, die bestimmten Kriterien entsprechen, herausgefiltert werden: Beispielsweise lassen sich mit einer Regel Ereignisse von geringerer Bedeutung und als „Noise“ identifizierte Events herausfiltern.
- je nach Schwere des Ereignisses Warnungen und Aktionen erfolgen: Wird ein Ereignis als „kritisch““ eingestuft, kann beispielsweise eine Warnung per SMS und E-Mail verschickt werden. Bei einer niedrigeren Klassifizierung wie „hoch“ besteht hingegen die Möglichkeit, die Mitteilung lediglich per E-Mail zu verschicken. Weitere Informationen hierzu erhalten Sie im Kapitel „Konfigurieren von Warnungen und Aktionen".
- gefilterte Ereignisse archiviert werden (optional): Die Archivierung erfolgt abhängig von der Schwere eines Ereignisses und den Einstellungen der Verarbeitungsregeln. Beispielsweise lassen sich nur solche Ereignisse für die Archivierung bestimmen, die als „kritisch“ oder „hoch“ klassifiziert wurden.

GFI EventsManager verwaltet Regeln zur Ereignisverarbeitung in Regelsätzen, in denen eine oder mehrere Einzelregeln gruppiert sein können.



Screenshot 38 – Ordner mit Regelsätzen und einzelne Regelsätze

Regelsätze werden in nach Kontrollbereich unterteilten Ordnern verwaltet. Je nach Kontrollbereich enthalten Regelsätze Regeln mit unterschiedlichen Funktionen und Aktionen. GFI EventsManager bietet bereits vordefinierte Regelsatz-Ordner, Regelsätze und Regeln zur Ereignisverarbeitung, die sich an Ihre Anforderungen anpassen lassen.

Ereignisklassifizierung

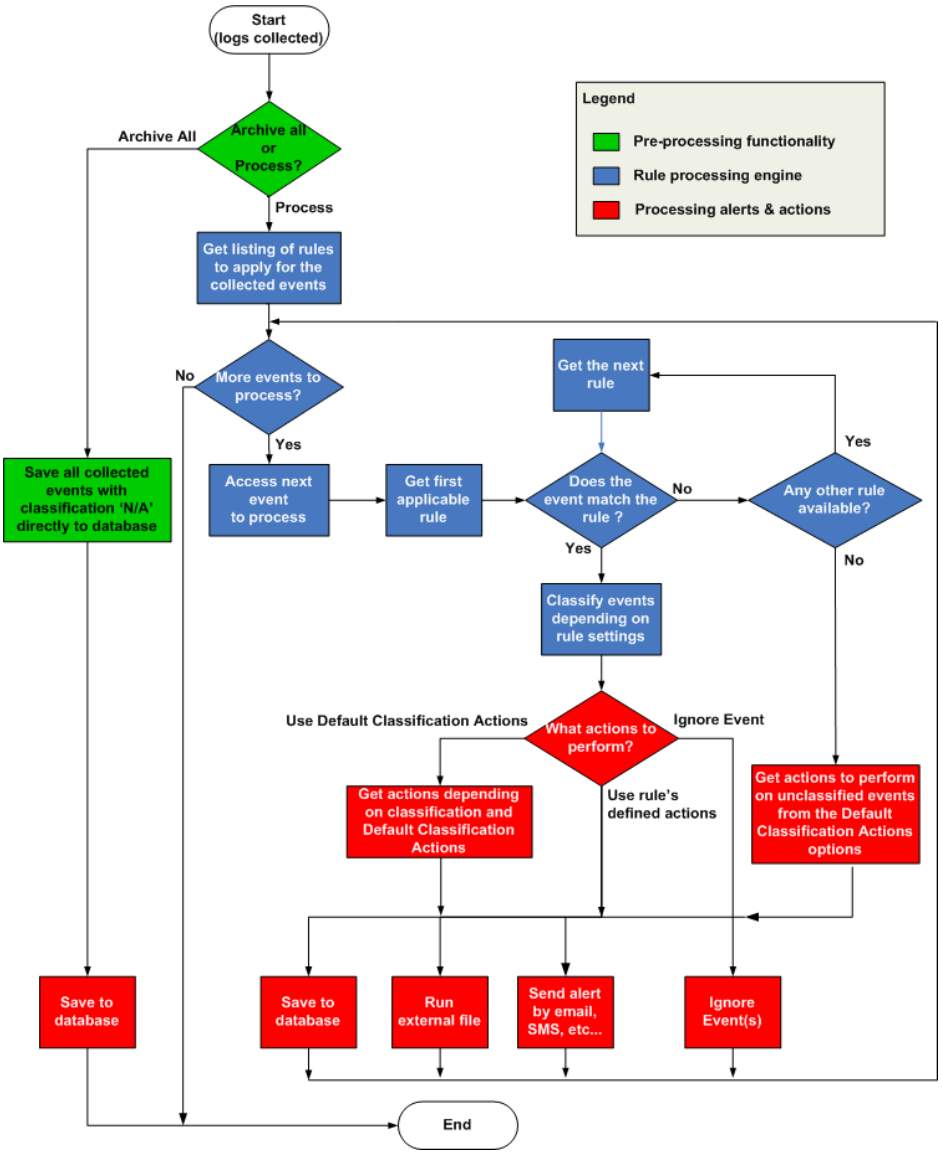
GFI EventsManager stuft Ereignisse in 5 Kategorien ein:

- Kritisch
- Hoch
- Mittel
- Niedrig
- Noise („Rauschen“, d. h. unerwünschte oder wiederholt auftretende Protokolleinträge)

Die Klassifizierung erfolgt anhand der auf die Protokolle angewendeten Regeln. Ereignisse, die keine Bedingungen der Regeln zur Ereignisklassifizierung erfüllen, werden als „nicht klassifiziert“ („unclassified“) gekennzeichnet. Auch für diese Ereignisse lassen sich dieselben Warnungen und Aktionen wie für klassifizierte Events einrichten.

Flussdiagramm zur Ereignisverarbeitung, Klassifizierung und zu Aktionen

Im folgenden Flussdiagramm werden die einzelnen Schritte der Ereignisverarbeitung durch GFI EventsManager dargestellt.

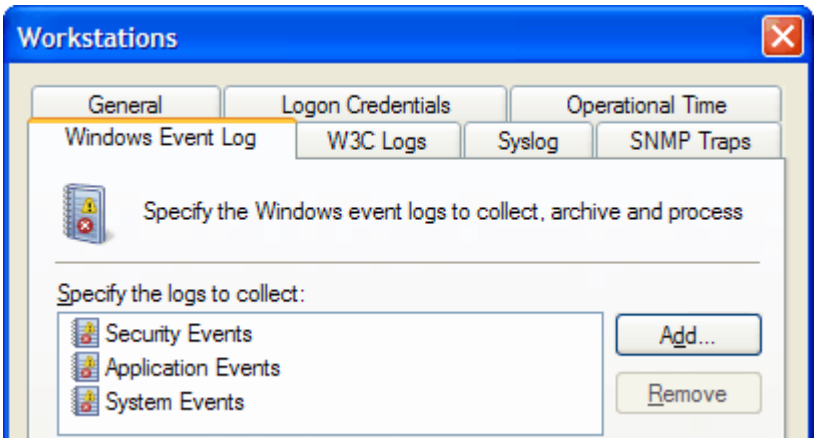


Screenshot 39 – Flussdiagramm zur Ereignisverarbeitung, Klassifizierung und zu Aktionen

Erfassen und Verarbeiten von Windows-Ereignisprotokollen

Überblick

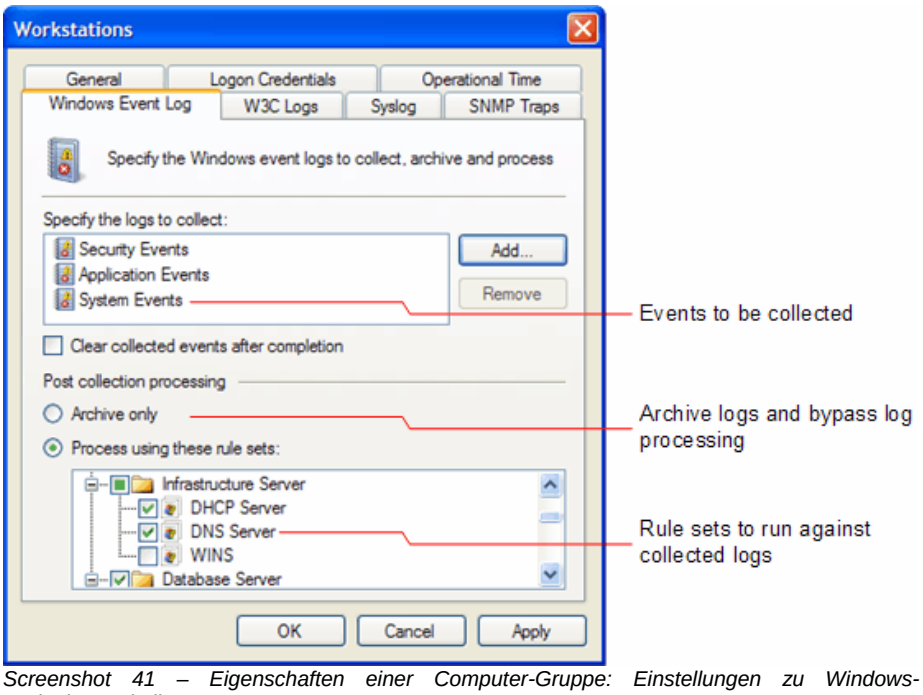
Windows-Ereignisse werden in unterschiedlichen Protokolltypen gesichert: Computer mit Windows NT oder höher erfassen Fehler, Warnungen und Informationen im Sicherheitsprotokoll, Anwendungsprotokoll bzw. Systemprotokoll. Zusätzlich zeichnen Computer mit besonderen Aufgaben im Netzwerk, beispielsweise Domänen-Controller und DNS-Server, Ereignisse in eigenen Protokollen auf.



Screenshot 40 – Eigenschaften einer Computer-Gruppe: zu verarbeitende Protokolle

Windows-Betriebssysteme zeichnen Ereignisse vorrangig in folgenden Protokollen auf:

- **Sicherheitsprotokoll:** Enthält sicherheitsrelevante Ereignisse, die sich zur Überwachung erfolgreicher oder versuchter Sicherheitsverletzungen nutzen lassen. Im Sicherheitsprotokoll werden beispielsweise gültige und ungültige Anmeldeversuche aufgezeichnet.
- **Anwendungsprotokoll:** Enthält Ereignisse, die von Programmen protokolliert wurden, beispielsweise Dateifehler.
- **Systemprotokoll:** Enthält Ereignisse, die von Windows XP-Systemkomponenten protokolliert wurden, beispielsweise Fehler beim Laden von Gerätetreibern beim Systemstart.
- **Verzeichnisdienstprotokoll:** Enthält von Active Directory (AD) ausgegebene Ereignisse, z. B. zur erfolgreichen oder fehlgeschlagenen Aktualisierung der AD-Datenbank.
- **Dateireplikationsdienst-Protokoll:** Enthält vom Windows-Dateireplikationsdienst protokollierte Ereignisse. Hierzu zählen fehlgeschlagene Dateireplikationen und Ereignisse während der Aktualisierung von Domänen-Controllern mit Sysvol-Daten.
- **DNS-Server-Protokoll:** Enthält Ereignisse zur Auflösung von DNS-Namen in IP-Adressen.
- **Anwendungs- und Dienstprotokolle:** Enthalten Ereignisse zu Windows Vista und den Diensten/Funktionalitäten des Betriebssystems.



Screenshot 41 – Eigenschaften einer Computer-Gruppe: Einstellungen zu Windows-Ereignisprotokollen

Folgende Einstellungen sind zur Erfassung und Verarbeitung von Windows-Ereignisprotokollen festzulegen:

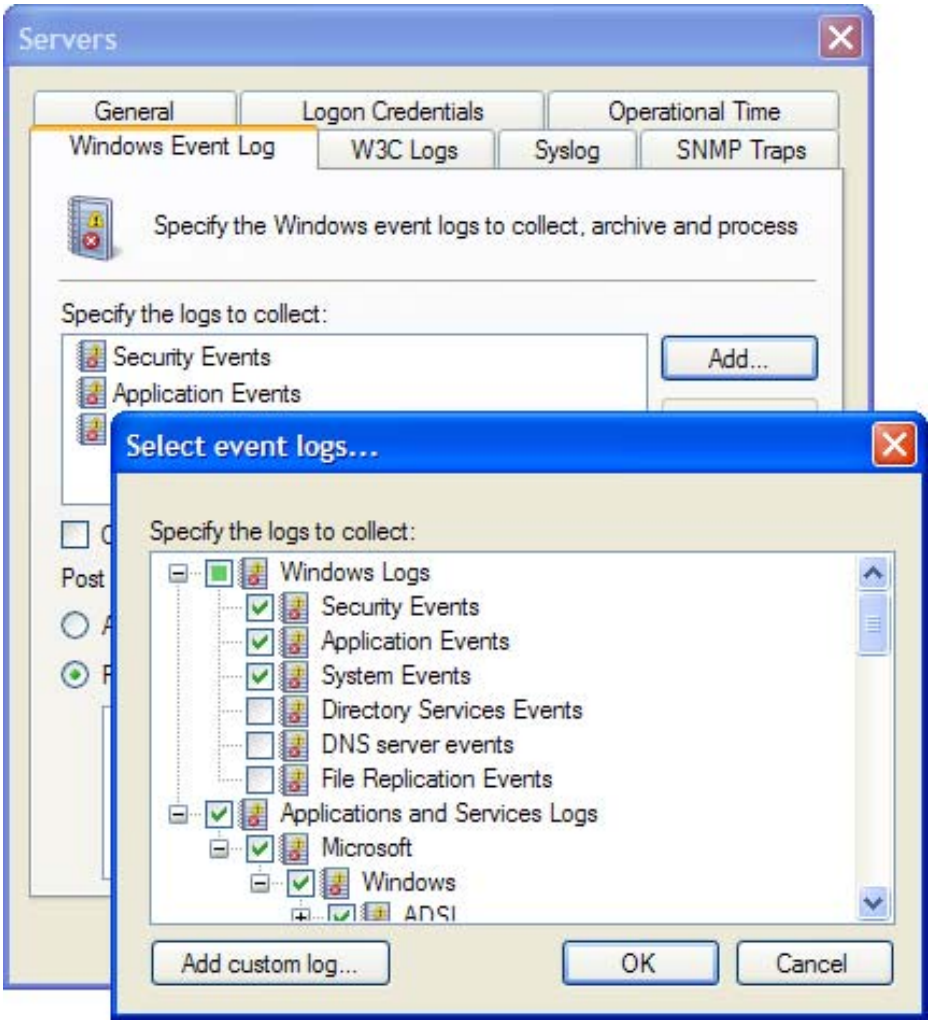
- Angabe der zu erfassenden Ereignisprotokolle
- Festlegung der Verarbeitung von Protokollen (z. B. Filterung) oder der Archivierung im Originalzustand
- Auswahl der Regelsätze/Regeln zur Ereignisverarbeitung, mit denen erfasste Protokolle kontrolliert werden sollen

Auswählen zu erfassender und zu bearbeitender Ereignis-protokolle

So legen Sie fest, welche Windows-Ereignisprotokolle von GFI EventsManager erfasst werden sollen:

1. Öffnen Sie den Eigenschaften-Dialog zum betreffenden Computer/zur Computer-Gruppe.

2. Klicken Sie auf den Reiter **Windows Event Log**.



Screenshot 42 – Auswählen zu erfassender Ereignisprotokolle

3. Klicken Sie auf die Schaltfläche **Add** und markieren Sie die zu erfassenden Protokolle.

Hinweis: GFI EventsManager unterstützt die Erfassung individueller Ereignisprotokolle. Weitere Informationen hierzu erhalten Sie in diesem Kapitel unter „Konfigurieren individueller Ereignisprotokolle".

4. Optional können Sie die Option **Clear collected events after completion** auswählen, um bereits erfasste Ereignisse von der Ereignisquelle zu löschen.

Wichtig: Beachten Sie, dass das Löschen von Ereignissen aus Protokollen der Ereignisquelle ohne vorherige Archivierung oder anderweitige Sicherung eine Verletzung gesetzlicher Richtlinien darstellen kann. Stellen Sie daher sicher, dass wichtige Ereignisse gemäß den für Ihr Unternehmen geltenden Gesetzen zur Daten-aufbewahrung und zum Datenschutz archiviert oder gesichert werden.

Archivieren von Windows-Ereignissen

Weitere Informationen zur Archivierung von Ereignissen erhalten Sie unter „Archivieren von Ereignissen“ in diesem Kapitel.

Auswählen von Regeln zur Verarbeitung von Windows-Ereignissen

Weitere Informationen zur Auswahl von Regeln zur Ereignisverarbeitung erhalten Sie unter „Auswählen von Regeln zur Ereignisverarbeitung“ in diesem Kapitel.

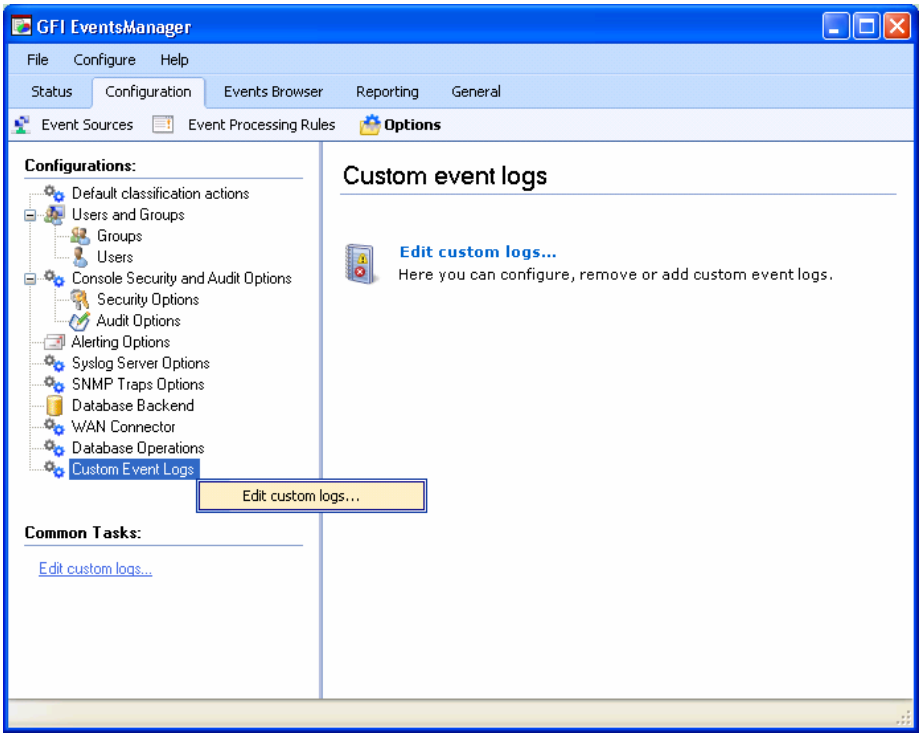
Konfigurieren individueller Ereignisprotokolle

Neben der Erfassung und Verarbeitung standardmäßiger Windows-Ereignisprotokolle kann GFI EventsManager auch Ereignisse verwalten, die in Protokollen von Drittanbieter-Lösungen erfasst wurden, beispielsweise von Anti-Virus-Lösungen, Software-Firewalls und anderen Sicherheitsprodukten.

So konfigurieren Sie die Bearbeitung individueller Ereignisprotokolle:

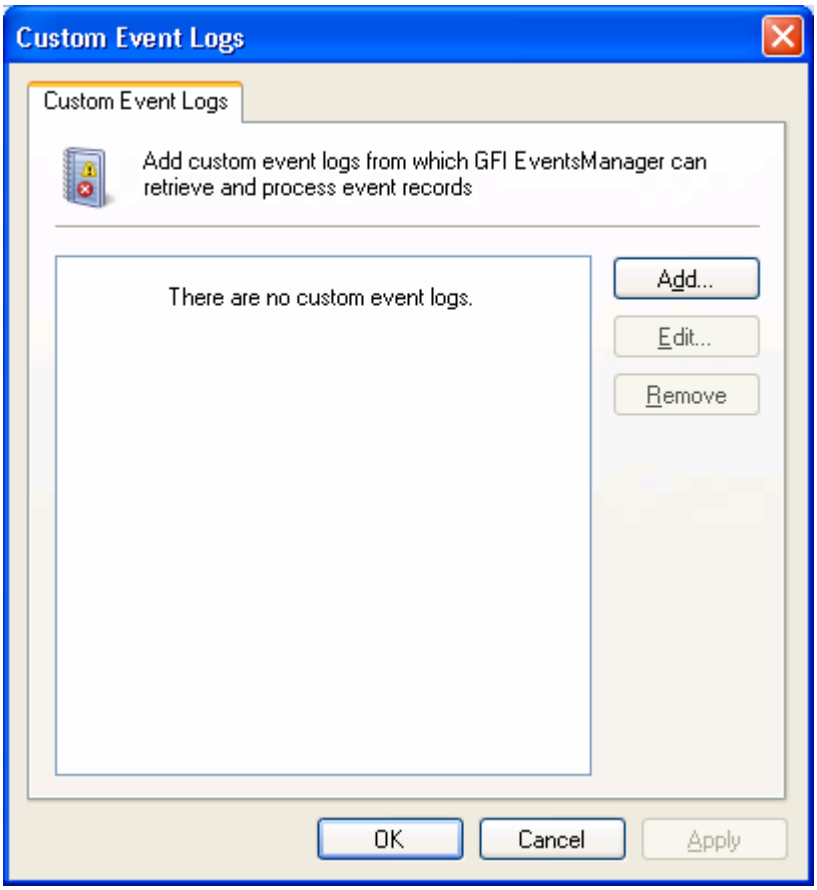
1. Klicken Sie auf den Reiter **Configuration** ▸ **Options**.

2. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf den Knoten **Custom Event Logs** und wählen Sie im Kontextmenü **Edit custom logs**.



Screenshot 43 – Festlegung individueller Ereignisprotokolle

3. Klicken Sie auf die Schaltfläche **Add** und geben Sie den Namen des Protokolls an.



Screenshot 44 – Hinzufügen eines individuellen Ereignisprotokolls

4. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen fertig zu stellen.

Erfassen und Verarbeiten von W3C-Protokollen

W3C-Protokolle sind textbasierte Flat-Files mit Ereignisdaten, die durch Sonderzeichen getrennt sind.

W3C-Protokolle werden vorrangig von Hardware-Systemen (z. B. Servern) genutzt, die besondere Aufgaben bei der Internet-Kommunikation übernehmen. Zum Beispiel erfassen Microsoft Internet Information Services (IIS) und Apache-Webserver Web-bezogene Ereignisse in Textdateien im W3C-Format.

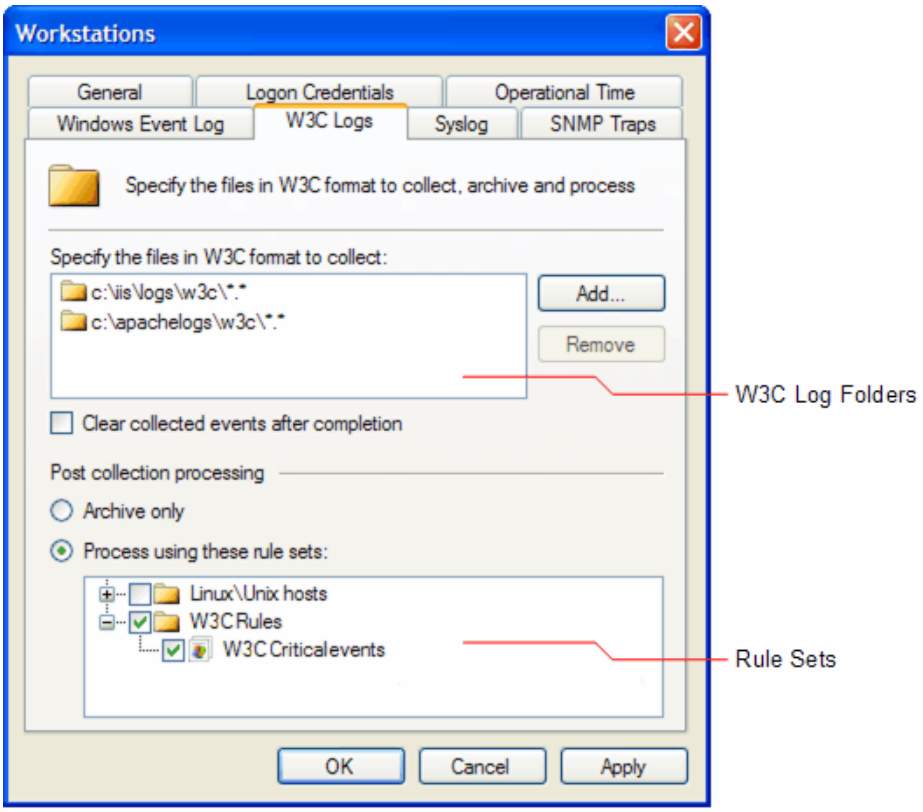
Die Festlegung der Parameter von W3C-Protokollen mit GFI EventsManager erfolgt analog zur Angabe der Einstellungen für Windows-Protokolle, mit einer Ausnahme: Im Gegensatz zu Windows-Ereignisprotokollen besteht keine Vorgabe zum Speicherort der Protokolldateien. Bei W3C-Protokollen muss daher der vollständige Speicherpfad angegeben werden.

Auswählen zu erfassender und zu verarbeitender Ereignis-protokolle

So legen Sie fest, welche W3C-Protokolle von GFI EventsManager erfasst werden sollen:

1. Öffnen Sie den Eigenschaften-Dialog zum betreffenden Computer/zur Computer-Gruppe.

2. Klicken Sie auf den Reiter **W3C Logs**.



Screenshot 45 – Eigenschaften einer Computer-Gruppe: Festlegen von Parametern zur Verarbeitung von W3C-Protokollen

3. Klicken Sie auf die Schaltfläche **Add** und geben Sie Name und Speicherort der Protokolldatei an. Bei der Eingabe können Platzhalter wie *.* verwendet werden.

4. Optional können Sie die Option **Clear collected events after completion** auswählen, um bereits erfasste Ereignisse von der Ereignisquelle zu löschen.

Wichtig: Beachten Sie, dass das Löschen von Ereignissen aus Protokollen der Ereignisquelle ohne vorherige Archivierung oder anderweitige Sicherung eine Verletzung gesetzlicher Richtlinien darstellen kann. Stellen Sie daher sicher, dass wichtige Ereignisse gemäß den für Ihr Unternehmen geltenden Gesetzen zur Datenaufbewahrung und zum Datenschutz archiviert oder gesichert werden.

Archivieren von W3C-Ereignissen

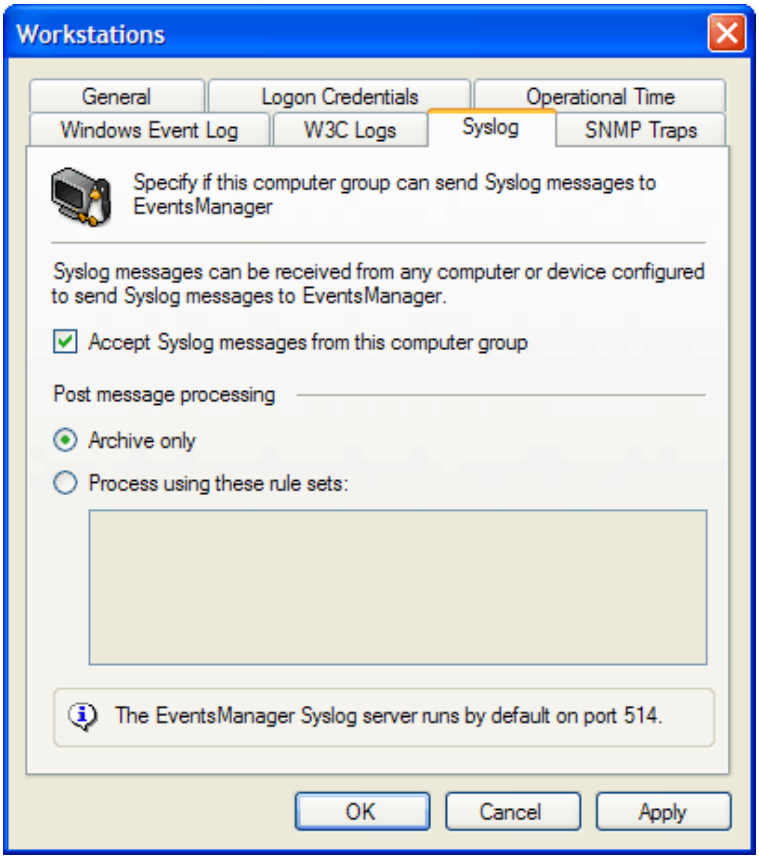
Weitere Informationen zur Archivierung von Ereignissen erhalten Sie unter „Archivieren von Ereignissen“ in diesem Kapitel.

Auswählen von Regeln zur Verarbeitung von W3C-Ereignissen

Weitere Informationen zur Auswahl von Regeln zur Ereignisverarbeitung erhalten Sie unter „Auswählen von Regeln zur Ereignisverarbeitung“ in diesem Kapitel.

Erfassen und Verarbeiten von Syslog-Meldungen

Syslog kommt vorrangig bei Linux- und Unix-Systemen zur Protokollierung von Ereignisdaten zum Einsatz. Die Protokollierung wird dabei vollständig von einem dedizierten Syslog-Server übernommen. Im Gegensatz zu Umgebungen mit Windows- und W3C-Protokollen erfolgt sie somit nicht durch die eigentlichen Programme. Ereignisinformationen werden lediglich als Datenmitteilungen (Syslog-Meldungen) an den Syslog-Server geschickt, der für die Verwaltung und Speicherung der Daten in einer Protokolldatei verantwortlich ist.


Workstations
General
Logon Credentials
Operational Time
Windows Event Log
W3C Logs
Syslog
SNMP Traps
Specify if this computer group can send Syslog messages to EventsManager
Syslog messages can be received from any computer or device configured to send Syslog messages to EventsManager.
Accept Syslog messages from this computer group
Post message processing
Archive only
Process using these rule sets:
The EventsManager Syslog server runs by default on port 514.
OK
Cancel
Apply

Screenshot 46 – Eigenschaften einer Computer-Gruppe: Parameter zur Verarbeitung von Syslog-Meldungen

Zur Verarbeitung von Syslog-Meldungen bietet GFI EventsManager einen integrierten Syslog-Server. Er erfasst automatisch sämtliche von Syslog-Quellen ausgegebenen Meldungen in Echtzeit und leitet sie zur Ereignisverarbeitung an die GFI EventsManager-Engine weiter. Standardmäßig werden ohne weitere Konfigurierung Ereignisse unterschiedlicher Netzwerk-Hardware, z. B. von Cisco und Juniper, unterstützt. Weitere Informationen zu den durch vorkonfigurierte Regeln unterstützten Geräten erhalten Sie in folgendem Knowledge-Base-Artikel von GFI:
http://kbase.gfi.com/showarticle.asp?id=KBID002868.

Durch einen integrierten Pufferspeicher kann der Syslog-Server bis zu 30 Meldungen zwecks Stapelverarbeitung erfassen, in eine Warteschlange stellen und weiterleiten. Zwischengespeicherte Meldungen werden standardmäßig an die Verarbeitungs-Engine weitergeleitet, wenn der Pufferspeicher seine maximale Kapazität erreicht hat oder in Intervallen von 1 Minute (je nachdem, welche dieser beiden Bedingungen zuerst eintritt).

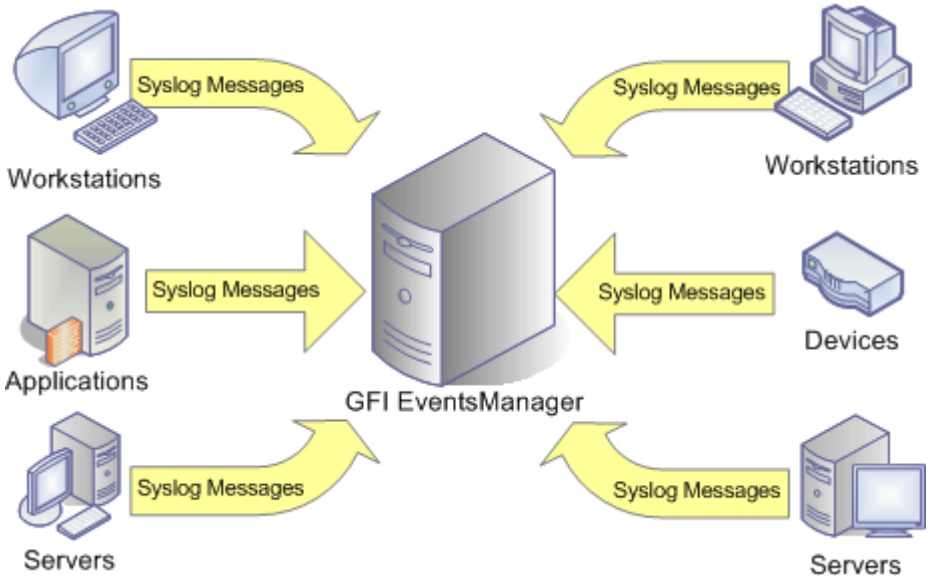


Abbildung 6 – Weiterleitung von Syslog-Meldungen an den GFI EventsManager-Computer

Hinweis: Zur korrekten Verarbeitung von Syslog-Meldungen müssen *alle* Syslog-Quellen (z. B. Workstations, Server, Netzwerkgeräte u. Ä.) so konfiguriert werden, dass sie die Informationen an den GFI EventsManager-Computer schicken. Diese Einstellung ist auch für den eigentlichen Computer, auf dem GFI EventsManager läuft, erforderlich.

So konfigurieren Sie die Einstellungen zur Verarbeitung von Syslog-Ereignissen in GFI EventsManager:

1. Öffnen Sie den jeweiligen Eigenschaften-Dialog zum betreffenden Computer/zur Computer-Gruppe.

2. Klicken Sie auf den Reiter **Syslog**.

3. Wählen Sie die Option **Accept Syslog messages from this computer group**, um den Syslog-Server für den Empfang von Meldungen dieser Computer-Gruppe zu aktivieren.

Wichtig: Beachten Sie, dass das Löschen von Ereignissen aus Protokollen der Ereignisquelle ohne vorherige Archivierung oder anderweitige Sicherung eine Verletzung gesetzlicher Richtlinien darstellen kann. Stellen Sie daher sicher, dass wichtige Ereignisse gemäß den für Ihr Unternehmen geltenden Gesetzen zur Datenaufbewahrung und zum Datenschutz archiviert oder gesichert werden.

Hinweis 1: Standardmäßig lauscht der Syslog-Server von GFI EventsManager auf Port 514 nach Syslog-Meldungen. Weitere Informationen zur Anpassung der Port-Einstellungen erhalten Sie unter „Konfigurieren des Syslog-Server-Ports“ in diesem Kapitel.

Hinweis 2: Der integrierte Syslog-Server akzeptiert nur Syslog-Meldungen von Computern, die zur gewählten Gruppe gehören.

Archivieren von Syslog-Ereignissen

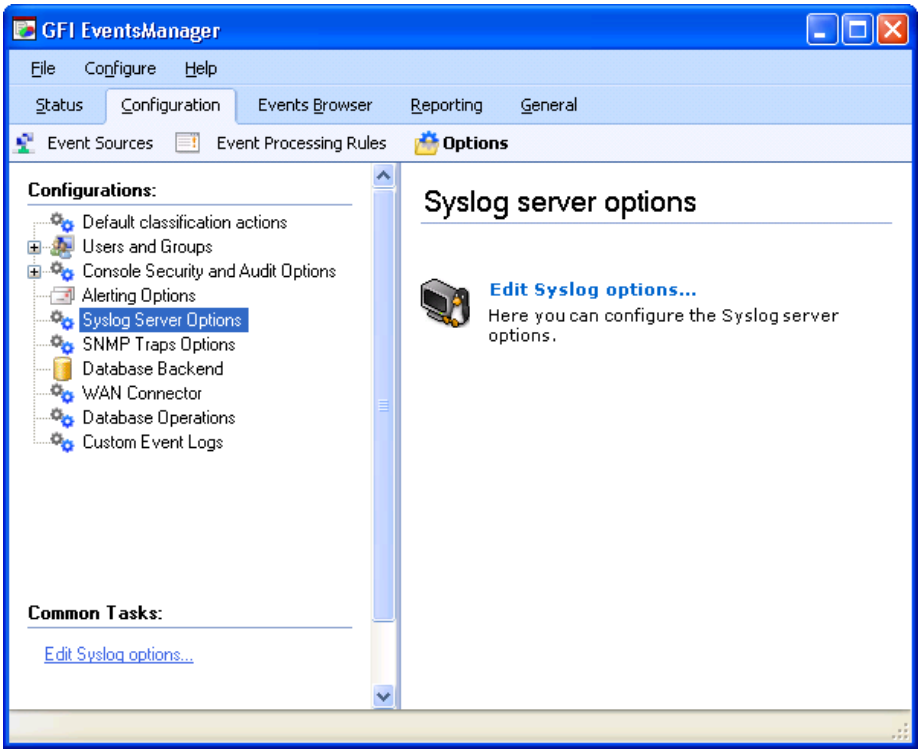
Weitere Informationen zur Archivierung von Ereignissen erhalten Sie unter „Archivieren von Ereignissen“ in diesem Kapitel.

Auswählen von Regeln zur Verarbeitung von Syslog-Ereignissen

Weitere Informationen zur Auswahl von Regeln zur Ereignisverarbeitung erhalten Sie unter „Auswählen von Regeln zur Ereignisverarbeitung“ in diesem Kapitel.

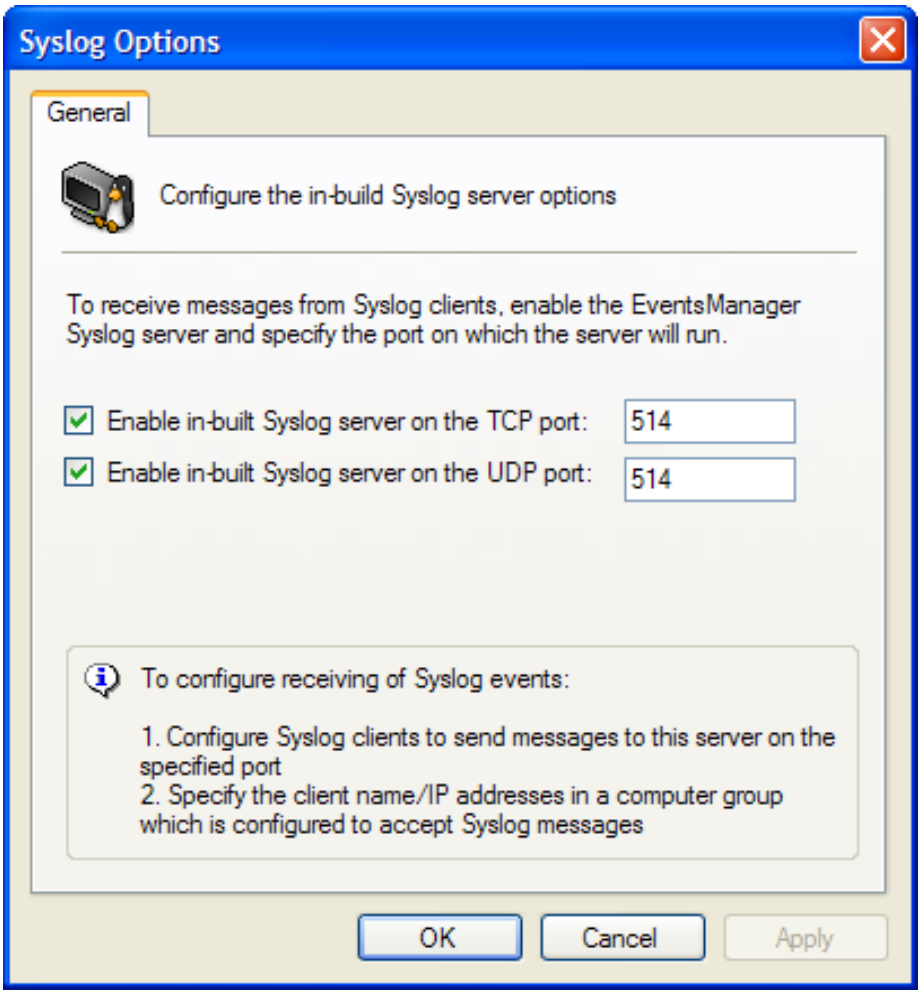
Konfigurieren des Syslog-Server-Ports

So ändern Sie den vorgegebenen Syslog-Port (TCP und UDP):



Screenshot 47 – Konfigurierung des Syslog-Servers

1. Klicken Sie auf den Reiter **Configuration**.
2. Klicken Sie auf **Options**.
3. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf den Knoten **Syslog Server Options** und wählen Sie im Kontextmenü **Edit Syslog options …**


Syslog Options
General
Configure the in-build Syslog server options
To receive messages from Syslog clients, enable the EventsManager Syslog server and specify the port on which the server will run.
Enable in-built Syslog server on the TCP port:
514
Enable in-built Syslog server on the UDP port:
514
To configure receiving of Syslog events:
1. Configure Syslog clients to send messages to this server on the specified port
2. Specify the client name/IP addresses in a computer group which is configured to accept Syslog messages
OK
Cancel
Apply

Screenshot 48 – Optionen des Syslog-Servers

4. Wählen Sie die Optionen **Enable in-built Syslog server on the [TCP]/[UDP] port** aus und geben Sie den TCP- und UDP-Port an, auf dem GFI EventsManager nach Syslog-Meldungen lauscht und diese empfängt.

5. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen zu speichern.

Hinweis: Stellen Sie sicher, dass die für den Syslog-Server angegebenen Ports nicht bereits von anderen installierten Anwendungen verwendet werden. Andernfalls könnte die Übermittlung von Syslog-Meldungen an GFI EventsManager beeinträchtigt werden.

Erfassen und Verarbeiten von SNMP-Traps

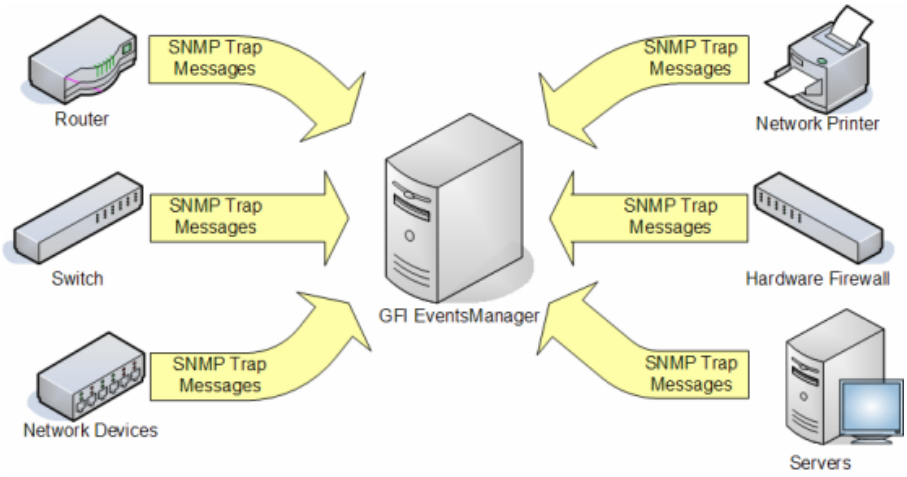
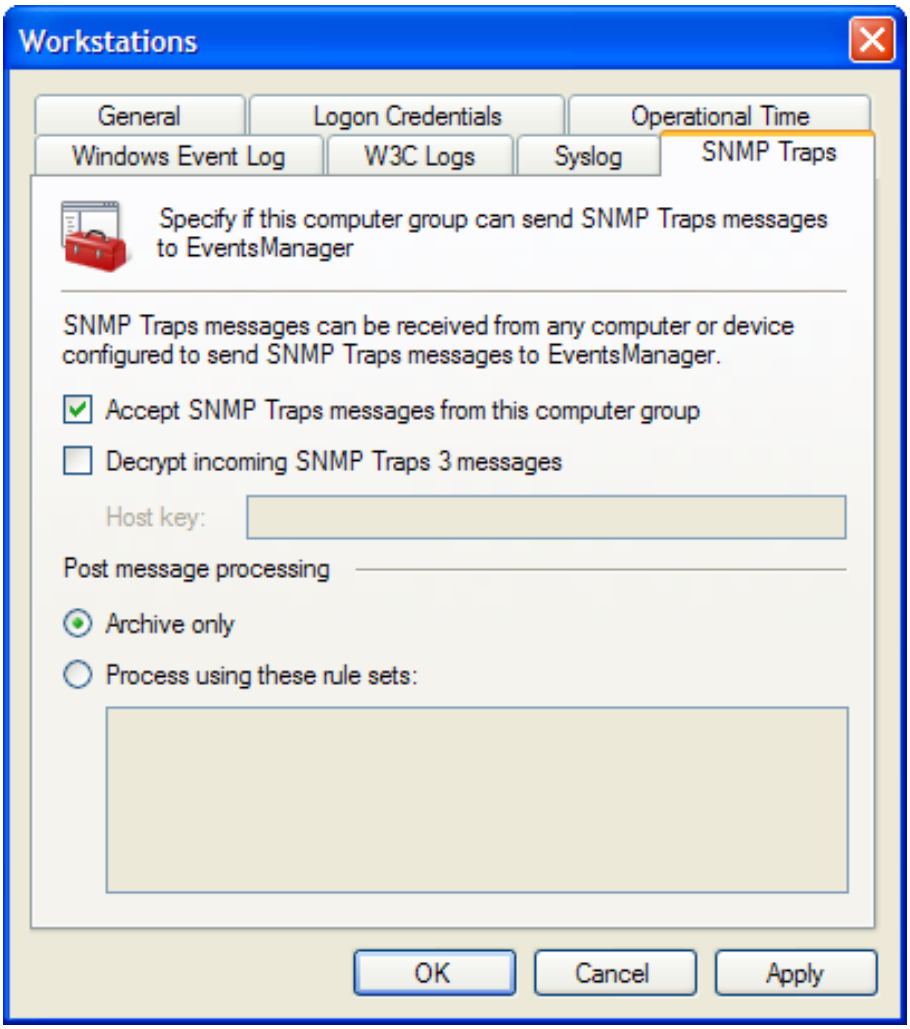


Abbildung 7 – Weiterleitung von SNMP-Traps an den GFI EventsManager-Computer

SNMP (Simple Network Management Protocol) ist ein Netzwerkprotokoll, mit dem Netzwerkelemente wie Router, Switches, Server u. Ä. zentral überwacht und gesteuert werden können. Auf netzwerkfähigen Geräten eingetretene Ereignisse werden von der Hardware per SNMP-Trap gemeldet und zur zentralen Protokollierung an einen SNMP-Trap-Server geschickt. Das SNMP-Messaging ähnelt somit dem Syslog-Konzept, da im Gegensatz zu Umgebungen mit Windows- und W3C-Protokollen die Hardware ihre SNMP-Meldungen nicht in lokalen Protokollen speichert.

GFI EventsManager bietet native Unterstützung für zahlreiche SNMP-fähige Geräte und zugehörige MIBs (Management Information Bases). Eine vollständige Liste der unterstützten Geräte steht zum Abruf bereit unter: http://kbase.gfi.com/showarticle.asp?id=KBID002868.



Screenshot 49 – Eigenschaften einer Computer-Gruppe: Parameter zur Verarbeitung von SNMP-Traps

Der für die Verarbeitung von SNMP-Traps erforderliche dedizierte SNMP-Trap-Server ist im Lieferumfang von GFI EventsManager enthalten. Durch einen integrierten Pufferspeicher kann er bis zu 30 Meldungen zwecks Stapelverarbeitung erfassen, in eine Warteschlange stellen und weiterleiten. Zwischengespeicherte Meldungen werden standardmäßig an die Verarbeitungs-Engine weitergeleitet, wenn der Pufferspeicher seine maximale Kapazität erreicht hat oder in Intervallen von 1 Minute (je nachdem, welche dieser beiden Bedingungen zuerst eintritt).

Hinweis: Zur korrekten Verarbeitung von SNMP-Traps müssen *alle* SNMP-Trap-Quellen (z. B. Workstations, Server, Netzwerkgeräte u. Ä.) so konfiguriert werden, dass sie Meldungen an den GFI EventsManager-Computer schicken. Diese Einstellung ist auch für den eigentlichen Rechner, auf dem GFI EventsManager läuft, erforderlich.

So legen Sie die Einstellungen zur Verarbeitung von SNMP-Traps fest:

1. Öffnen Sie den Eigenschaften-Dialog zum betreffenden Computer/zur Computer-Gruppe.

2. Klicken Sie auf den Reiter **SNMP-Traps**.

3. Zum Empfang und zur Verarbeitung von SNMP-Traps per SNMP-Trap-Server wählen Sie die Option **Accept SNMP Traps messages from this computer group**.

Wichtig: Beachten Sie, dass das Löschen von Ereignissen aus Protokollen der Ereignisquelle ohne vorherige Archivierung oder anderweitige Sicherung eine Verletzung gesetzlicher Richtlinien darstellen kann.

Hinweis 1: Standardmäßig lauscht der SNMP-Trap-Server von GFI EventsManager auf Port 162 nach SNMP-Traps. Weitere Informationen zur Anpassung der Port-Einstellungen erhalten Sie unter „Konfigurieren der Einstellungen des SNMP-Trap-Servers" in diesem Kapitel.

Hinweis 2: Der SNMP-Trap-Server akzeptiert nur SNMP-Meldungen von Computern, die zur gewählten Gruppe gehören.

Hinweis 3: Der SNMP-Trap-Server unterstützt auch verschlüsselte Traps der SNMP-Version 3. Für diese Meldungen muss zur Entschlüsselung im Feld **Decrypt incoming SNMP Traps 3 messages** der Host-Schlüssel angegeben werden.

Archivieren von SNMP-Traps

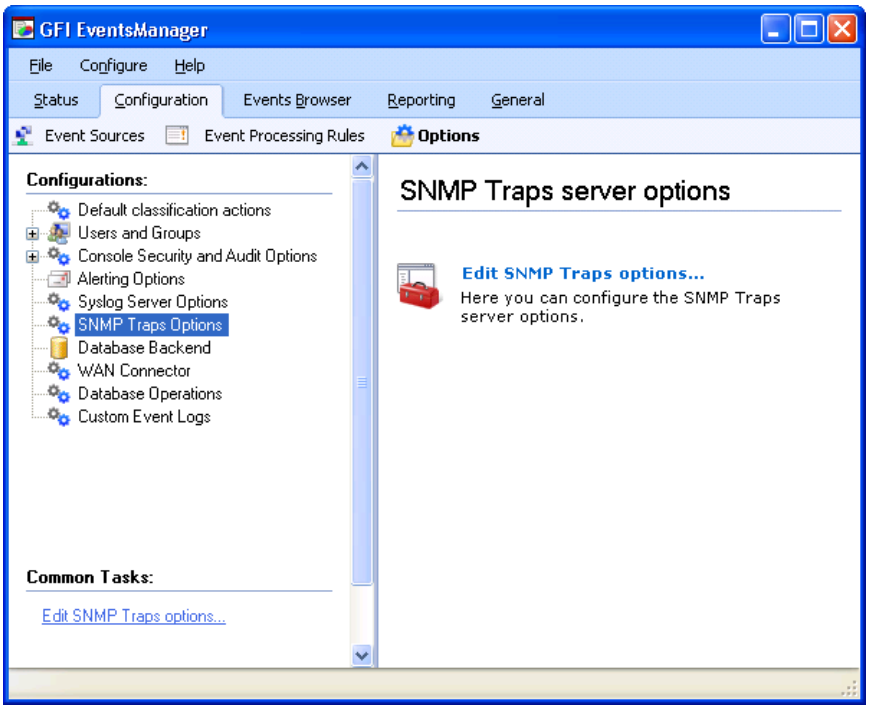
Weitere Informationen zur Archivierung von Ereignissen erhalten Sie unter „Archivieren von Ereignissen“ in diesem Kapitel.

Auswählen von Regeln zur Verarbeitung von SNMP-Traps

Weitere Informationen zur Auswahl von Regeln zur Ereignisverarbeitung erhalten Sie unter „Auswählen von Regeln zur Ereignisverarbeitung“ in diesem Kapitel.

Konfigurieren der Einstellungen des SNMP-Trap-Servers

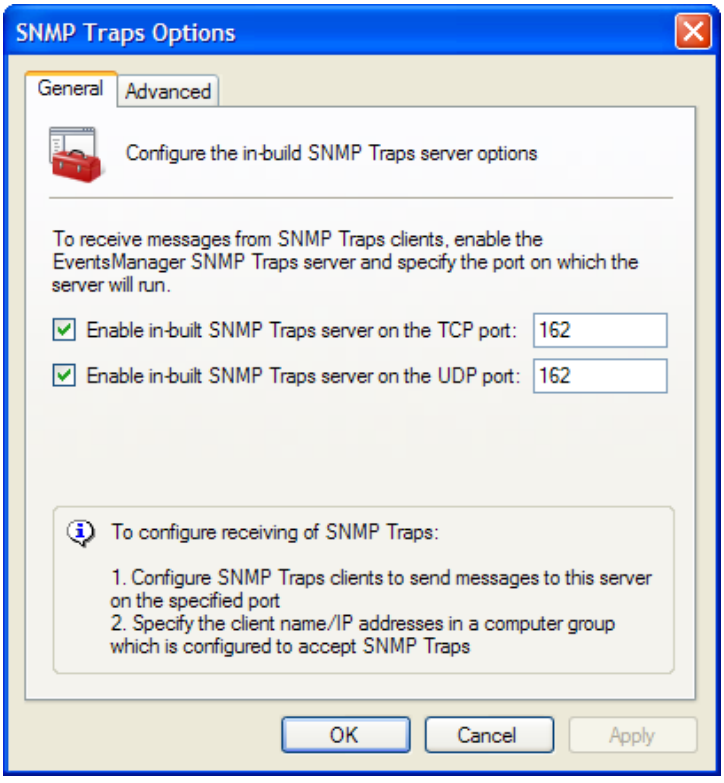
So ändern Sie die standardmäßigen Einstellungen des SNMP-Trap-Servers:



Screenshot 50 – Konfigurieren des SNMP-Trap-Servers

1. Klicken Sie auf den Reiter **Configuration** ▸ **Options**.

2. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf den Knoten **SNMP Traps Options** und wählen Sie **Edit SNMP Traps options.**


SNMP Traps Options
General
Advanced
Configure the in-build SNMP Traps server options
To receive messages from SNMP Traps clients, enable the EventsManager SNMP Traps server and specify the port on which the server will run.
Enable in-built SNMP Traps server on the TCP port:
162
Enable in-built SNMP Traps server on the UDP port:
162
To configure receiving of SNMP Traps:
1. Configure SNMP Traps clients to send messages to this server on the specified port
2. Specify the client name/IP addresses in a computer group which is configured to accept SNMP Traps
OK
Cancel
Apply

Screenshot 51 – Optionen des SNMP-Trap-Servers

3. Wählen Sie die Optionen **Enable in-built SNMP Traps server on the [TCP]/[UDP] port** aus und geben Sie den TCP- und UDP-Port an, auf dem GFI EventsManager nach SNMP-Meldungen lauscht und diese empfängt.

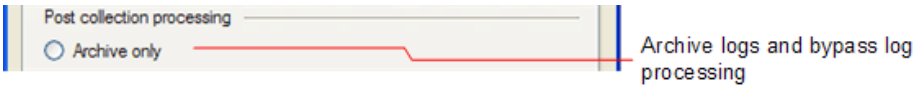
4. Klicken Sie auf den Reiter **Advanced**, falls Sie SNMP-Trap-OIDs (Object Identifiers) hinzufügen, bearbeiten oder entfernen möchten.

5. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen fertig zu stellen.

Hinweis: Stellen Sie sicher, dass die für den SNMP-Trap-Server angegebenen Ports nicht bereits von anderen installierten Anwendungen verwendet werden. Andernfalls könnte die Übermittlung von SNMP-Traps an GFI EventsManager beeinträchtigt werden.

Archivieren von Ereignissen

Archivieren von Ereignissen ohne Protokollverarbeitung



Screenshot 52 – Archivieren von Ereignissen ohne vorherige Verarbeitung

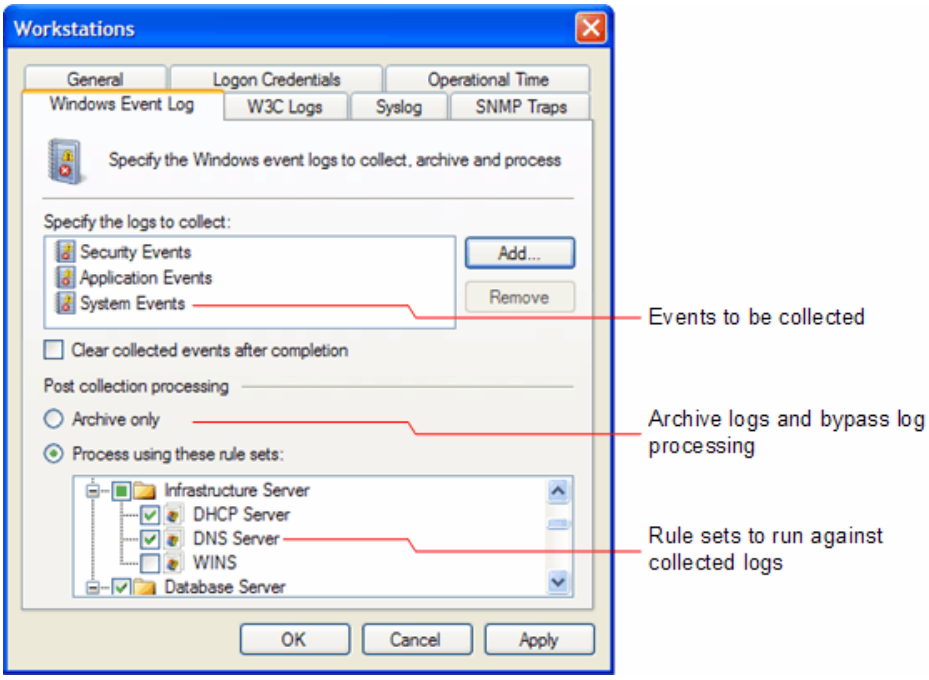
GFI EventsManager verarbeitet standardmäßig alle von den Zielrechnern abgerufenen Protokolle. Um Ereignisse unverarbeitet zu archivieren, wählen Sie für den jeweiligen Protokolltyp im Bereich **Post collection [messaging] processing** die Option **Archive only**.

Archivieren von Ereignissen nach der Verarbeitung

Verarbeitete Ereignisse lassen sich optional im Datenbank-Backend von GFI Events Manager archivieren. Die automatische Archivierung kann anhand folgender Kriterien erfolgen:

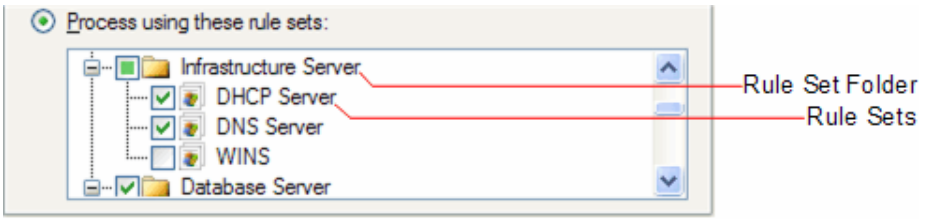
- unter Berücksichtigung der Ereignisklassifizierung. Sie können beispielsweise Standardeinstellungen festlegen, nach denen nur als „kritisch“ klassifizierte Ereignisse archiviert werden. Informationen zur Konfigurierung der Ereignisarchivierung für dieses Kriterium erhalten Sie im Kapitel „Konfigurieren von Warnungen und Aktionen" unter „Konfigurieren von standardmäßigen Klassifizierungsaktionen“.
- unter Berücksichtigung der in den Regeln zur Ereignisverarbeitung definierten Bedingungen. Verarbeitete Ereignisse lassen sich mit Hilfe von Regeln weitaus flexibler archivieren. So ist es möglich, nur solche Ereignisse zu sichern, die ungeachtet ihrer Klassifizierung bestimmte Bedingungen erfüllen. Beispielsweise können Sie eine Regel einrichten, die lediglich als „kritisch“ klassifizierte Ereignisse der Ereigniskennung 537 archiviert. Weitere Informationen zur Erstellung und Konfigurierung von Regeln zur Ereignisverarbeitung erhalten Sie im Kapitel „Konfigurieren von Regeln zur Ereignisverarbeitung“.

Auswählen von Regeln zur Ereignisverarbeitung



Screenshot 53 – Eigenschaften einer Computer-Gruppe: Einstellungen zu Windows-Ereignisprotokollen

Legen Sie fest, welche Regeln zur Verarbeitung und Klassifizierung der in Protokollen erfassten Ereignisse zur Anwendung kommen sollen. Wählen Sie hierfür den Regelsatz-Ordner oder einzelne Regelsätze aus, in denen die gewünschten Regeln zur Ereignis-verarbeitung enthalten sind.



Screenshot 54 – Auswahl der Regeln/Regelsätze zur Ereignisverarbeitung

Achten Sie darauf, dass Sie eine zum Protokoll passende Regel anwenden. Im Lieferumfang von GFI EventsManager enthaltene Regelsätze sind bereits für bestimmte Protokolltypen vorkonfiguriert. Um die Ereignisse aus den erfassten Protokollen wie gewünscht zu verarbeiten, müssen daher die richtigen Regelsätze ausgewählt werden.

Einige Sätze enthalten Regeln, die sich auf spezielle Ereignisse beziehen. Werden diese Regeln zur Verarbeitung anderer Ereignisse verwendet, sind eine fehlerhafte Verarbeitung, Datenverlust und irrelevante Ergebnisse die Folge. Beispiel: Der Regelsatz „Monitoring and Attack Detection“ umfasst Regeln, die speziell zur Verarbeitung von Windows-Sicherheitsereignissen konzipiert wurde. Eine Anwendung dieser Regel auf Anwendungsereignisse unter Windows liefert somit keine verwertbaren Ergebnisse.

Hinweis 1: GFI EventsManager wird standardmäßig mit vorausgewählten Regelsätzen/-ordnern bereitgestellt, die bereits eine

effektive Verarbeitung von Windows-Ereignisprotokollen erlauben. Sollten Sie mit dem Produkt oder der Verwendung von Regelsätzen noch nicht vertraut sein, empfiehlt GFI, die Standardeinstellungen beizubehalten.

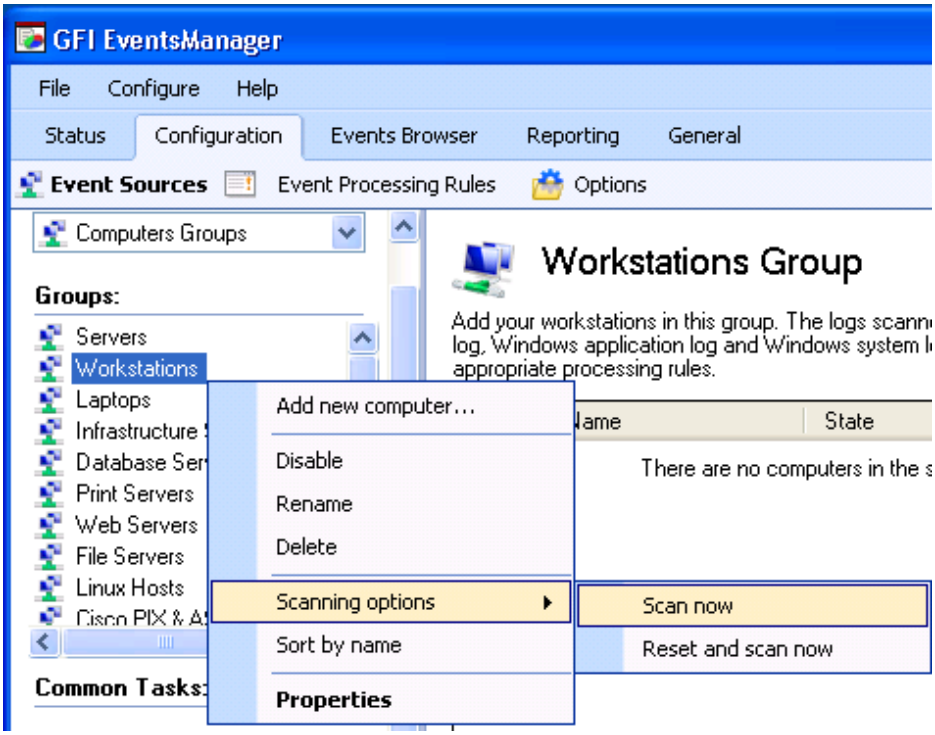
Hinweis 2: Werden im Auswahlbereich keine Regelsätze angezeigt, stehen für den aktuellen Protokolltyp keine Regeln zur Ereignisverarbeitung zur Verfügung. Weitere Informationen zur Konfigurierung von Regeln zur Ereignisverarbeitung und von Regelsätzen erhalten Sie im Kapitel „Konfigurieren von Regeln zur Ereignisverarbeitung“.

Manuelles Scannen von Ereignisquellen

Der Scan von Ereignisquellen kann umgehend manuell gestartet werden. Gehen Sie hierfür wie folgt vor:

1. Klicken Sie im linken Fensterbereich der Verwaltungskonsole mit der rechten Maustaste auf die Computer-Gruppe, in der sich die Quellen befinden.

2. Gehen Sie auf **Scanning options ▸ Scan now**, um den Scan der Gruppe sofort zu starten.



Screenshot 55 – Manuelles Scannen von Ereignisprotokollen

Konfigurieren von Warnungen und Aktionen

Einführung

Werden während der Verarbeitung von Ereignisprotokollen spezielle Ereignisse festgestellt, kann GFI EventsManager automatisch Aktionen durchführen. Hierzu zählen der Versand von E-Mail-Warnungen und die Archivierung von Ereignissen.

Warnungen und Aktionen lassen sich auf zwei Arten auslösen:

1. im Rahmen von klassifizierungsabhängigen Standardaktionen („Default Classification Actions“)

2. durch die Erstellung oder Anpassung von Regeln und Regelsätzen.

Default Classification Actions (klassifizierungsabhängige Standardaktionen)

Anhand der über die **Default Classification Actions** festlegbaren Einstellungen können Warnungen und Aktionen allein auf Grundlage der Klassifizierung eines Ereignisses ausgelöst werden. Im Rahmen dieser Kontrolle lassen sich Parameter festlegen, mit denen beispielsweise E-Mail-Warnungen für sämtliche als „kritisch“, „hoch“, „mittel“ und „niedrig“ klassifizierten Ereignisse erfolgen, jedoch nur als „kritisch“ gekennzeichnete Events archiviert werden.

Von Regeln zur Ereignisverarbeitung gestartete Aktionen

Durch das Erstellen von Regeln lassen sich Aktionen noch differenzierter konfigurieren: Sie können gezielt ausgelöst werden, wenn ein Ereignis eine oder mehrere in den Regeln definierte Bedingungen erfüllt. Zum Beispiel kann eine Regel veranlassen, dass ein Ereignis ungeachtet seiner Klassifizierung nur dann archiviert wird, wenn es die Ereigniskennung 231 besitzt.

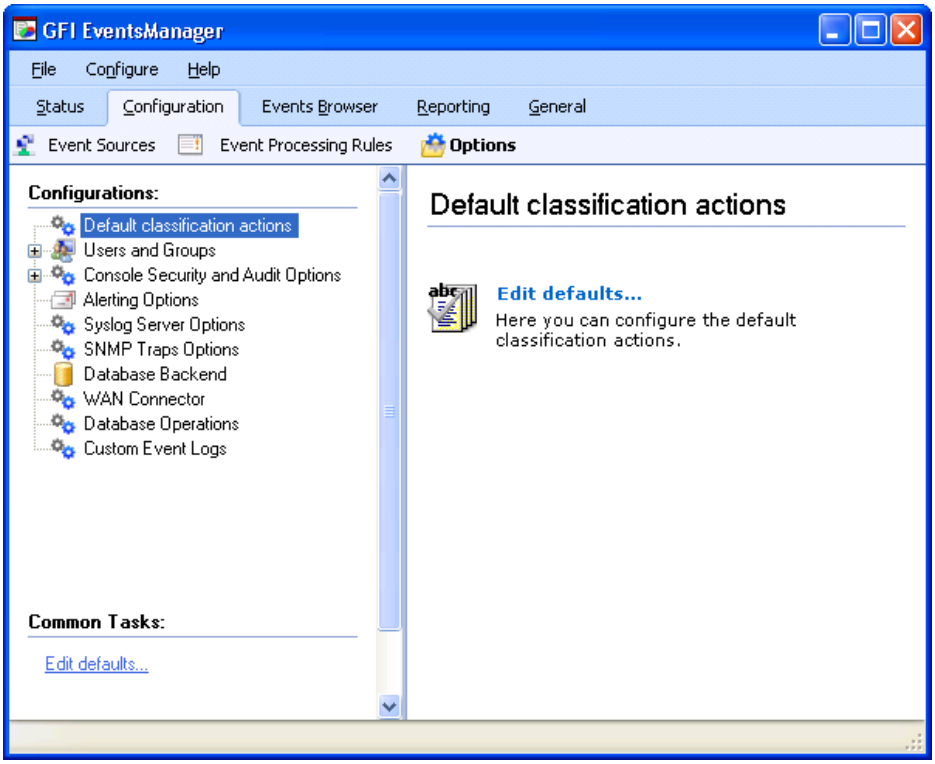
Unterstützte Aktionen

GFI EventsManager erlaubt die Durchführung folgender Aktionen:

- **Archivierung eines Ereignisses** – Ein klassifiziertes Ereignis wird per Aktion **Archive the event** im Datenbank-Backend von GFI EventsManager archiviert.
- **Versand von Warnungen per E-Mail/SMS/Netzwerk** – Warnungen lassen sich per Aktion **Send email/SMS/network notifications to** über verschiedene Kommunikationskanäle an Systemverantwortliche verschicken.

- **Öffnen einer Datei** – GFI EventsManager erlaubt per **Run File** das Starten einer ausführbaren Datei. Hierzu zählen VBScripts (.vbs), Batch-Dateien (.bat) und andere ausführbare Dateien (.exe). Zusätzlich lassen sich beliebige Befehlszeilen-parameter an ausführbare Dateien übergeben.

Konfigurieren der standardmäßigen Klassifizierungsaktionen

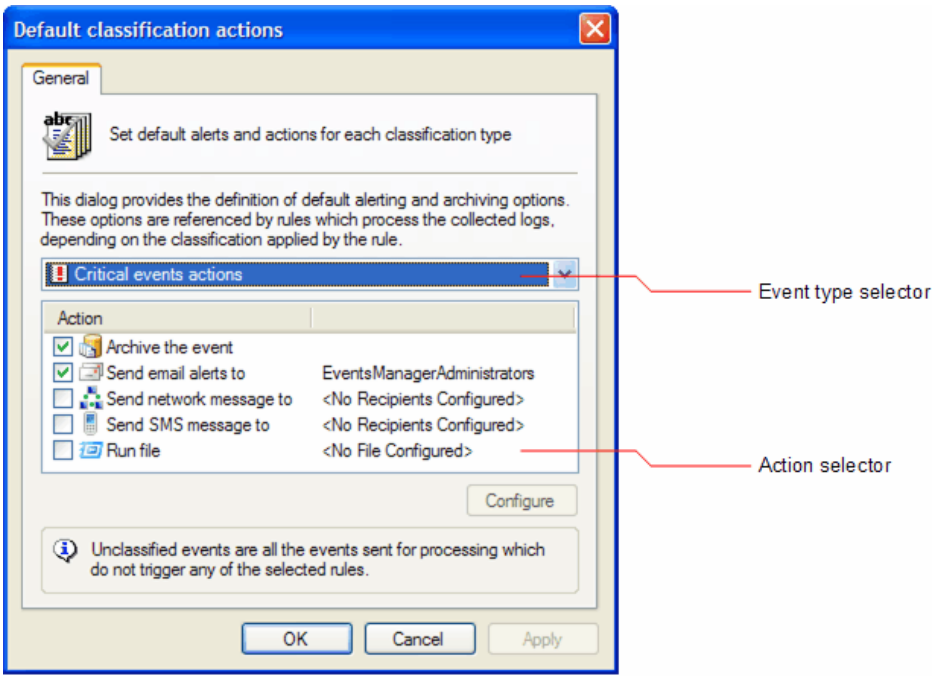


Screenshot 56 – Konfigurieren der standardmäßigen Klassifizierungsaktionen

So legen Sie die Einstellungen für die klassifizierungsabhängigen Standardaktionen (**Default Classification Actions**) fest:

1. Klicken Sie auf den Reiter **Configuration** ▸ **Options**.

2. Klicken Sie im linken Navigationsbereich mit der rechten Maustaste auf den Knoten **Default classifications actions** und wählen Sie im Kontextmenü **Edit defaults…**



Screenshot 57 – Klassifizierungsabhängige Aktionen

3. Wählen Sie aus der angezeigten Drop-Down-Liste die zu bearbeitende Ereignisklassifizierung aus.

4. Wählen Sie auf der Liste **Action** die Aktionen aus, die für die gewählte Ereignisklassifizierung ausgelöst werden sollen.

5. Klicken Sie auf die Schaltfläche **Configure**, um weitergehende Einstellungen für die jeweilige Aktion vorzunehmen.

Hinweis: Beachten Sie, dass Aktionen für als „niedrig“ klassifizierte Ereignisse folgende Auswirkungen haben können:

- Der Datenverkehr im Netzwerk wird erhöht (v. a. bei Warnungen per E-Mail, SMS oder Netzwerk).
- Im Fall einer Archivierung vergrößern sich der Datenaustausch mit der Backend-Datenbank und deren Wachstum bedeutend.

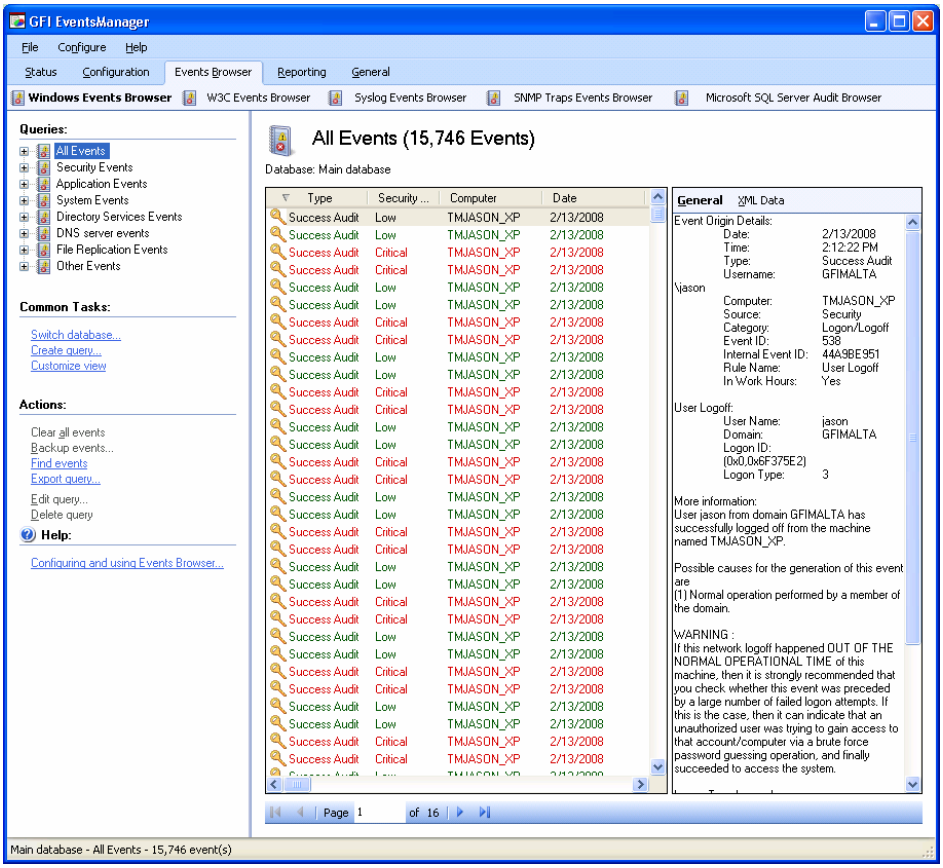
Konfigurieren von Aktionen für Regeln zur Ereignisverarbeitung

Weitere Informationen zur Konfigurierung und Auslösung von Aktionen im Rahmen von Regeln zur Ereignisverarbeitung erhalten Sie im Kapitel „Konfigurieren von Regeln zur Ereignisverarbeitung“.

Ereignisanzeige per Events-Browser

Einführung

Die über den Reiter **Events Browser** aufrufbaren Browser dienen der Darstellung verarbeiteter und unverarbeiteter Ereignisse/Protokolle, die im Datenbank-Backend oder in der Backup-Datenbank gespeichert sind.


GFI EventsManager
File Configure Help
Status Configuration Events Browser Reporting General
Windows Events Browser W3C Events Browser Syslog Events Browser SNMP Traps Events Browser Microsoft SQL Server Audit Browser
Queries:
All Events
Security Events
Application Events
System Events
Directory Services Events
DNS server events
File Replication Events
Other Events
Common Tasks:
Switch database...
Create query...
Customize view
Actions:
Clear all events
Backup events...
Find events
Export query...
Edit query...
Delete query
Help:
Configuring and using Events Browser...
All Events (15,746 Events)
Database: Main database
Type Security ... Computer Date
Success Audit Low TMJASON_XP 2/13/2008
Success Audit Critical TMJASON_XP 2/13/2008
General XML Data
Event Origin Details:
Date: 2/13/2008
Time: 2:12:22 PM
Type: Success Audit
Username: GFIMALTA
\jason
Computer: TMJASON_XP
Source: Security
Category: Logon/Logoff
Event ID: 538
Internal Event ID: 44A9BE951
Rule Name: User Logoff
In Work Hours: Yes
User Logoff:
User Name: jason
Domain: GFIMALTA
Logon ID: (0x0,0x6F375E2)
Logon Type: 3
More information:
User jason from domain GFIMALTA has successfully logged off from the machine named TMJASON_XP.
Possible causes for the generation of this event are
(1) Normal operation performed by a member of the domain.
WARNING :
If this network logoff happened OUT OF THE NORMAL OPERATIONAL TIME of this machine, then it is strongly recommended that you check whether this event was preceded by a large number of failed logon attempts. If this is the case, then it can indicate that an unauthorized user was trying to gain access to that account/computer via a brute force password guessing operation, and finally succeeded to access the system.
Page 1 of 16
Main database - All Events - 15,746 event(s)

Screenshot 58 – Events Browser

Die verschiedenen Browser unterstützen zudem die digitale Spurensuche bei forensischen Analysen von Ereignissen. Sämtliche Ereignisse können nach Protokolltyp geordnet über fünf Browser-Reiter dargestellt werden: **Windows Events Browser**, **W3C Events Browser**, **Syslog Events Browser**, **SNMP Traps Browser** und **Microsoft SQL Server Audit Browser**. Ereignisse eines bestimmten Protokolltyps lassen sich hierdurch schneller aufrufen. Ereignisinformationen werden in Spalten angezeigt. Klicken Sie auf ein Ereignis, damit zusätzliche Hinweise in einem separaten Fensterbereich angezeigt werden.

Event ID: 532	
Source	adsctlr
Type	Warning
Description	Failed to connect to the device (device name: <name> IP address: <IP address>): Failed to connect to the remote computer because of certificate issues. Also check the date on the target computer.
Comments	Ionut Marin (Last update 10/2/2005): Microsoft has a hotfix that might solve this problem. See M875533 for details. Bryan Fowler (Last update 10/1/2005): In my case the BIOS date was incorrect. I corrected it and then I was able to connect to the deployment agent successfully.
Links	M875533
Search	Microsoft Support - Microsoft Search - Google Groups - Google Microsoft - EventID.Net Queue - More links...
Various	Send comments - Notify me when updated

Screenshot 59 – Ereignisdetails

Detaillierte Informationen zu Windows-Ereignissen sind über zwei Reiter im rechten Fensterbereich abrufbar:

- Reiter **General –** Liefert Informationen im Format, das vor der Einführung von Microsoft Windows Vista für Ereignisprotokolle verwendet wurde.
- Reiter **XML Data –** Liefert Informationen im neuen XML-basierten Ereignisprotokolll-Format von Microsoft Windows Vista.

Klicken Sie auf den in den Ereignisbeschreibungen angezeigten Link, um folgende Informationen aufzurufen:

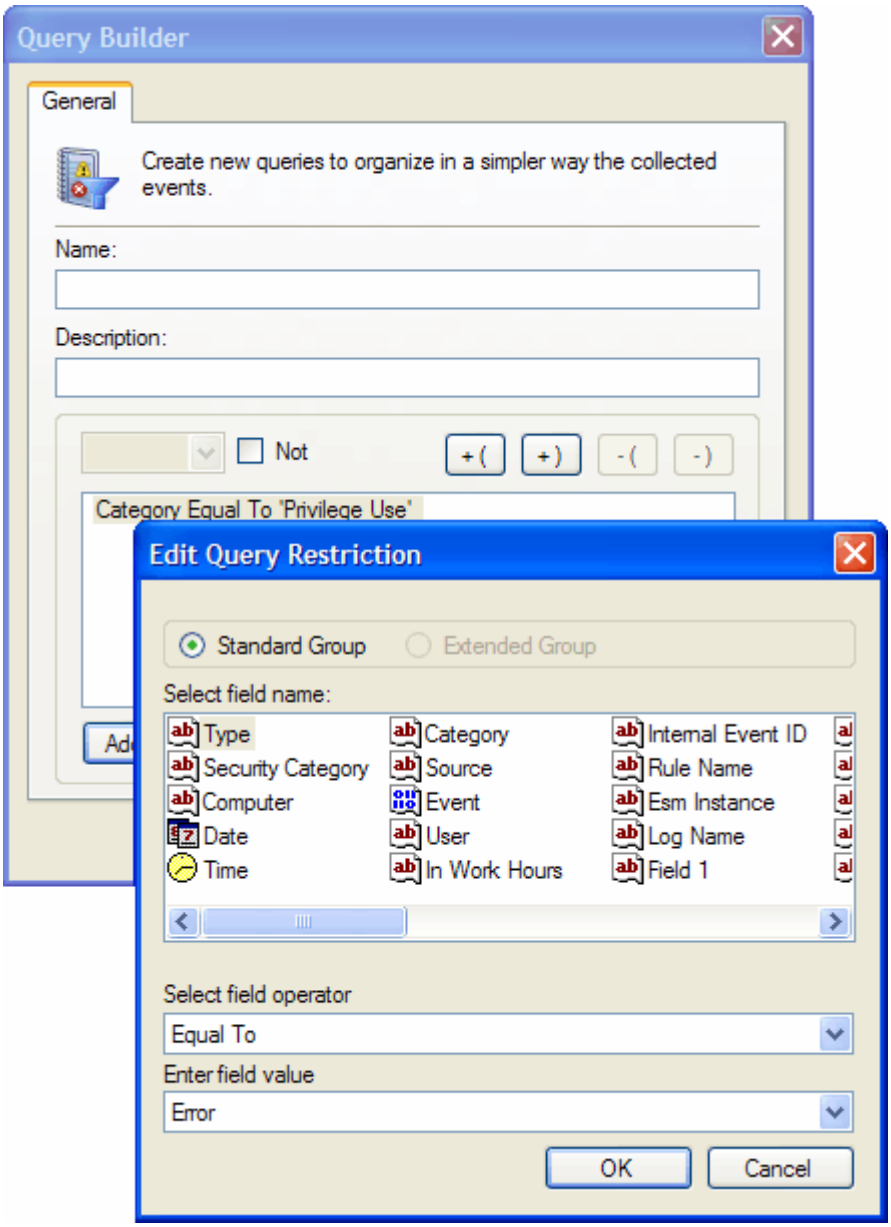
- eine umfangreichere Beschreibung des Ereignisses
- Hinweise und Links zu Ursachen des Ereignisses
- Weitergehende Hinweise und Lösungsvorschläge zu Problemen

Tools zur Ereignisanzeige

Spezialwerkzeuge von GFI EventsManager vereinfachen das Durchsuchen und Anzeigen von Ereignissen sowie deren Export in CSV-Dateien. Zu diesen Tools gehören:

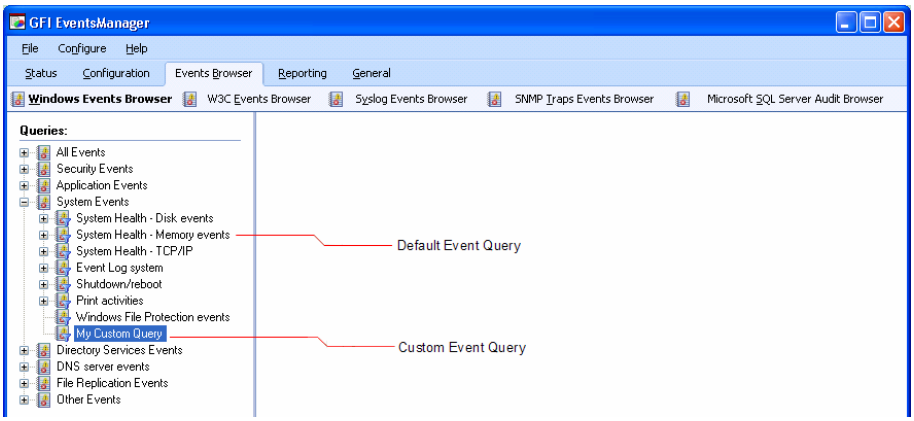
- ein Ereignisfilter/Ereignisabfrage-Generator
- farbliches Hervorheben unterschiedlicher Ereignisse
- Tool zur Ereignissuche
- Tool zum Export von Ereignissen

Ereignisfilter/Ereignisabfrage-Generator



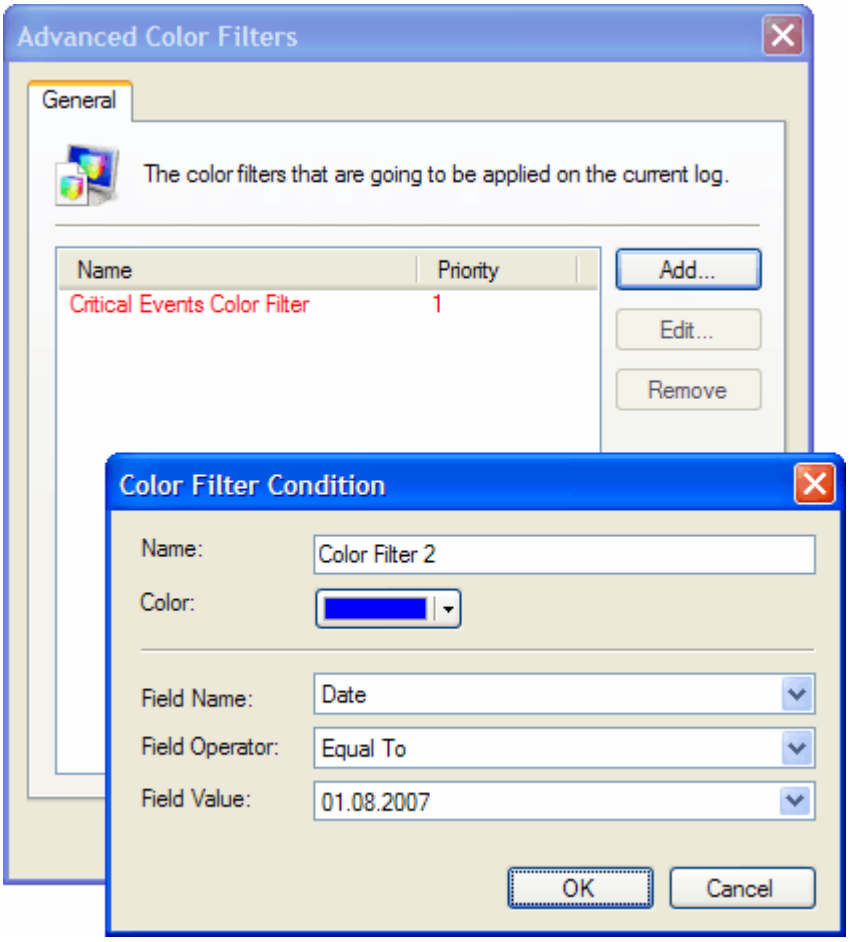
Screenshot 60 – Generator für Ereignisabfragen

Mit Hilfe des Ereignisabfrage-Generators lassen sich eigene Filter zur separaten Darstellung spezieller Ereignisse einrichten, ohne dass diese aus dem Datenbank-Backend gelöscht werden. Diese Filter können zusätzlich zur bereits im Lieferumfang enthaltenen Standard-auswahl, die keine weitere Konfigurierung erfordert, eingesetzt werden.



Screenshot 61 – Standardmäßige und benutzerdefinierte Ereignisabfragen

Farbliches Hervorheben unterschiedlicher Ereignisse



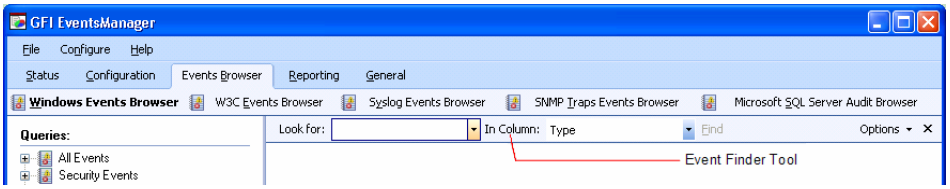
Screenshot 62 – Filter zur farblichen Kennzeichnung des Gefährdungsgrads

Mit Hilfe des Tools zur Ereigniskennzeichnung lassen sich Ereignisse ihrem Gefährdungsgrad entsprechend farblich kennzeichnen. Eine solche Markierung erleichtert das schnelle Auffinden wichtiger Ereignisse bei der Durchsicht. Beispielsweise lässt sich eine Abfrage zu Ereignissen der Kategorie „kritisch“ oder „hoch“ erstellen, bei der zusätzlich alle kritischen Ereignisse der Kennung 231 rot gekennzeichnet werden.

Die Festlegung der Farbkodierung erfolgt über einen eigenen Abfragegenerator. Für diesen sind festzulegen:

- Bedingungen zur Kennzeichnung einzelner Ereignisse
- Auswahl der Farbe zur Hervorhebung

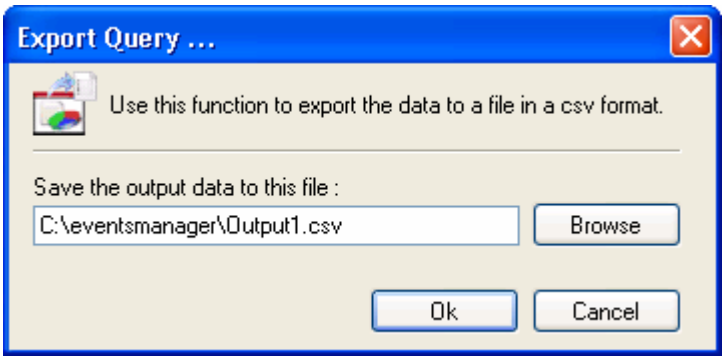
Tool zur Ereignissuche



Screenshot 63 – Tool zur Ereignissuche

Mit dem Tool zur Ereignissuche können Ereignisse gezielt anhand einzelner Abfragen gefunden werden. Zum Beispiel lassen sich Ereignisse mit einer speziellen Kennung anzeigen oder solche, deren Beschreibung bestimmte Stichwörter enthält.

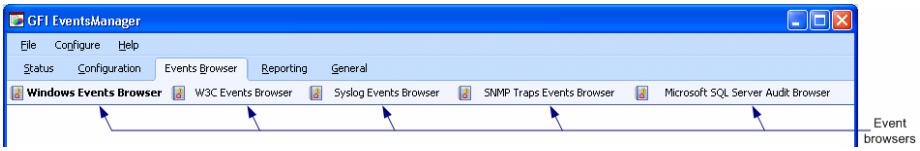
Tool zum Exportieren von Ereignissen


Export Query ...
Use this function to export the data to a file in a csv format.
Save the output data to this file :
C:\eventsmanager\Output1.csv
Browse
Ok
Cancel

Screenshot 64 – Tool zum Export von Ereignissen

Mit Hilfe des Tools zum Export von Ereignissen lassen sich Ereignisinformationen in CSV-Dateien sichern. Weitere Informationen hierzu erhalten Sie im Kapitel „Exportieren von Ereignissen“ in diesem Handbuch.

Anzeigen gespeicherter Ereignisprotokolle


GFI EventsManager
File Configure Help
Status Configuration Events Browser Reporting General
Windows Events Browser W3C Events Browser Syslog Events Browser SNMP Traps Events Browser Microsoft SQL Server Audit Browser
Event browsers

Screenshot 65 – Events Browser

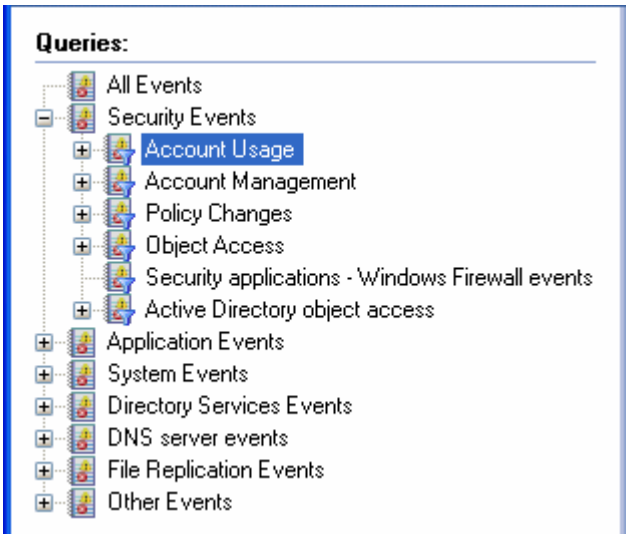
Klicken Sie auf den Reiter **Events Browser** und wählen Sie eine der fünf Browser-Kategorien aus, um im Datenbank-Backend gespeicherte Ereignisse anzuzeigen.

Starten einer Ereignisabfrage

Ereignisabfragen lassen sich bereits über die Anzeige per **Events Browser** starten:

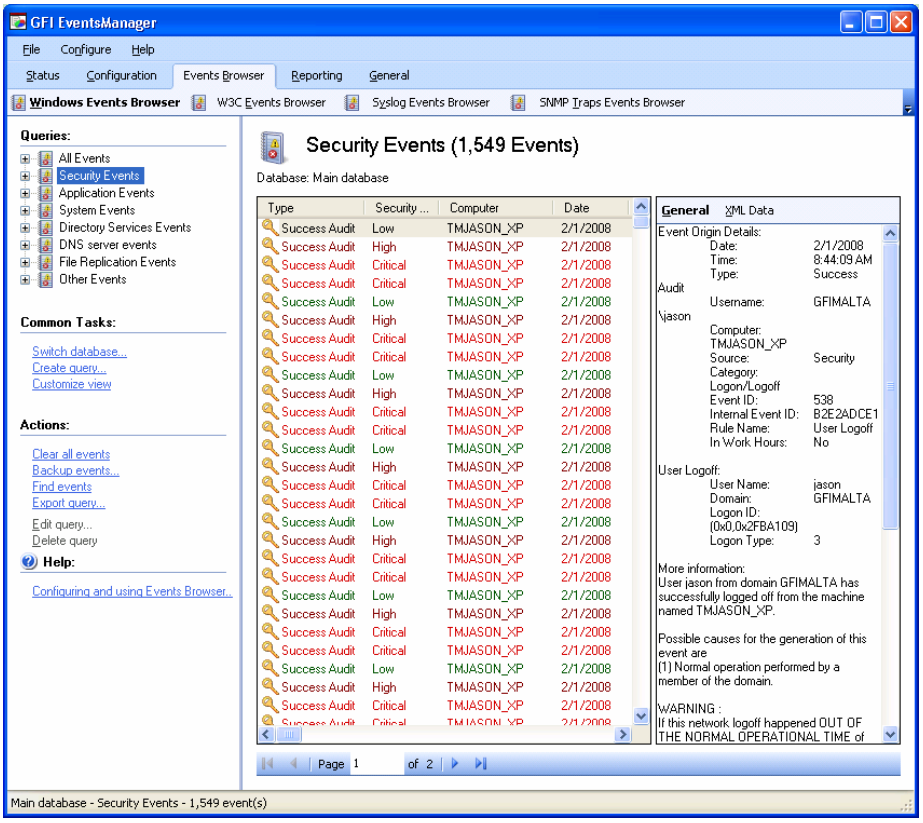
1. Klicken Sie auf den Reiter **Events Browser** und wählen Sie den gewünschten Browser aus.

2. Wählen Sie im linken Fensterbereich den gewünschten Ereignisfilter aus, z. B. **Account Usage** zur Kontenverwendung. Herausgefilterte Ereignisse werden im rechten Fenster angezeigt.



Screenshot – Filterauswahl

Erstellen benutzerdefinierter Ereignisabfragen

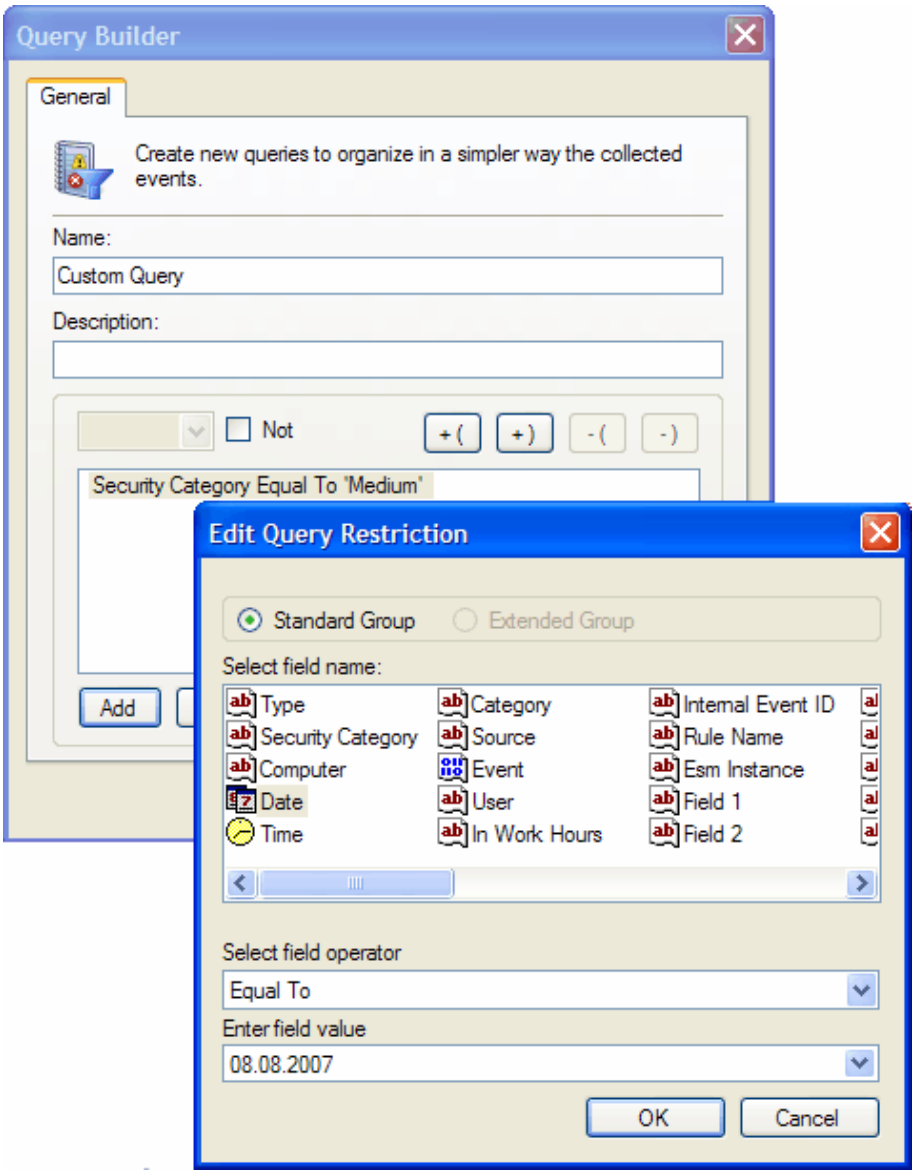


Screenshot 66 – Events Browser

Benutzerdefinierte Ereignisabfragen werden als Unterknoten zu bereits vorgegebenen Abfragen hinzugefügt. So erstellen Sie eine benutzerdefinierte Ereignisabfrage:

1. Klicken Sie auf den Reiter **Events Browser** und wählen Sie den gewünschten Browser aus.

2. Klicken Sie im linken Fensterbereich unter **Queries** mit der rechten Maustaste auf die Standardabfrage, unter der die neue Abfrage erstellt werden soll. Wählen Sie im Kontextmenü **Create query...**, um den Ereignisabfrage-Generator zu starten.



Screenshot 67 – Erstellung benutzerdefinierter Ereignisabfragen

3. Geben Sie Namen und Beschreibung der neuen Abfrage an.

4. Klicken Sie auf die Schaltfläche **Add**, um eine Abfragebedingung festzulegen. Klicken Sie danach auf die Schaltfläche **OK**. Wiederholen Sie diesen Schritt, bis alle erforderlichen Bedingungen angegeben sind.

5. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen fertig zu stellen.

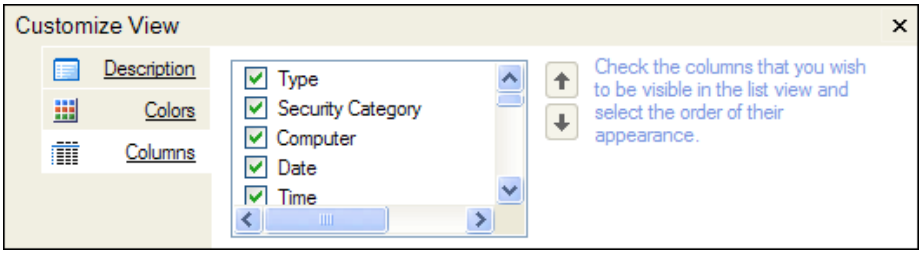
Anpassen des Ereignisanzeige-Bereichs

Auswählen der anzuzeigenden Spalten

So legen Sie fest, welche Spalten im Anzeigebereich eines Protokoll-Browsers dargestellt werden sollen:

1. Klicken Sie auf den Reiter **Events Browser** und wählen Sie den gewünschten Browser aus.

2. Wählen Sie im linken Fensterbereich unter **Common Tasks** die Option **Customize view** aus.



Screenshot 68 – Anpassung des Anzeigefensters: Spaltenauswahl

3. Klicken Sie im rechten Fensterbereich unter **Customize View** auf **Columns**.

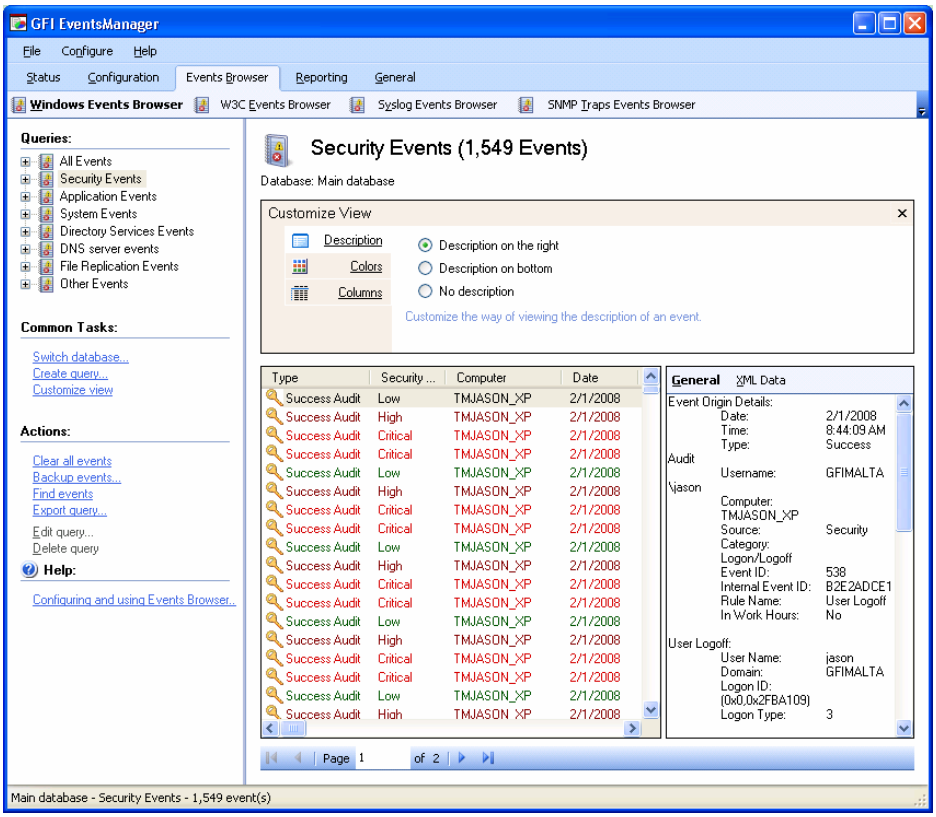
4. Wählen Sie alle Spalten aus, die im Ereignisanzeige-Fenster von GFI EventsManager dargestellt werden sollen. Mit Hilfe der Nach-oben- und Nach-unten-Pfeile können Sie festlegen, in welcher Reihenfolge Spalten anzuzeigen sind.

5. Schließen Sie das Fenster **Customize View**, um die Einstellungen zu speichern.

Anzeigen der Ereignisbeschreibung

So legen Sie fest, wo auf der rechten Seite des Ereignisanzeige-Bereichs die Beschreibung eines Ereignisses angezeigt werden soll:

1. Klicken Sie auf den Reiter **Events Browser** und wählen Sie den gewünschten Browser aus.



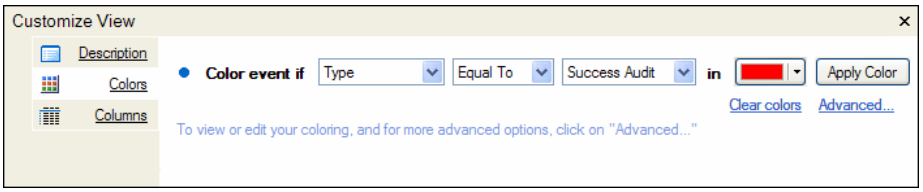
Screenshot 69 – Anpassung des Anzeige-Fensters

2. Klicken Sie im linken Fensterbereich im Bereich **Common Tasks** auf **Customize view**.

3. Klicken Sie im rechten Fensterbereich unter **Customize View** auf **Description** und passen Sie die Einstellungen wie gewünscht an.

Farbliches Kennzeichnen von Ereignissen

Kennzeichnen eines Ereignisses mit einer bestimmten Eigenschaft



Screenshot 70 – Farbliche Kennzeichnung eines Ereignisses

So können Sie Ereignisse mit einer bestimmten Eigenschaft farblich kennzeichnen:

1. Klicken Sie auf den Reiter **Events Browser** und wählen Sie den gewünschten Browser aus.

2. Wählen Sie im linken Fensterbereich unter **Common Tasks** die Option **Customize view** aus. Klicken Sie im rechten Fensterbereich unter **Customize View** auf **Colors**.

3. Geben Sie die Filtereinstellungen an und wählen Sie die Farbe aus, in der herausgefilterte Ereignisse gekennzeichnet werden sollen.

4. Klicken Sie auf die Schaltfläche **Apply Color**, um die Einstellungen zu speichern.

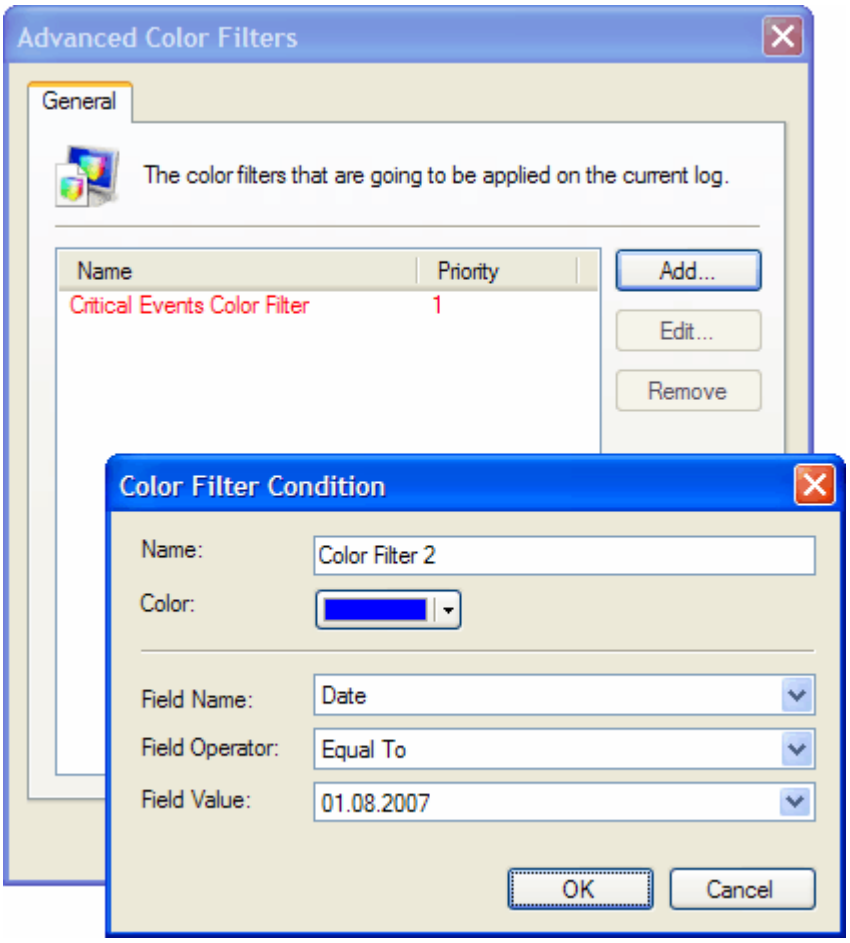
Hinweis: Sollen sämtliche Farbeinstellungen gelöscht werden, klicken Sie auf die Option **Clear color filters**.

Kennzeichnen mehrerer Ereignisse

So kennzeichnen Sie gleich mehrere Ereignisse mit unterschiedlichen Farben:

1. Klicken Sie auf den Reiter **Events Browser** und wählen Sie den gewünschten Browser aus.

2. Wählen Sie im linken Fensterbereich unter **Common Tasks** die Option **Customize view** aus. Klicken Sie im rechten Fensterbereich unter **Customize View** auf die Option **Colors** und auf **Advanced**.



Screenshot 71 – Erweiterte Optionen für Farbfilter

3. Klicken Sie im Dialog **Advanced Color Filters** auf die Schaltfläche **Add**. Benennen Sie den Filter und legen Sie die gewünschten Einstellungen fest.

4. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen zu speichern.

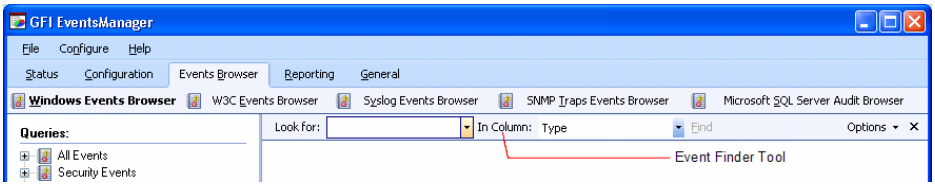
5. Wiederholen Sie diesen Schritt, bis alle Farbfilter festgelegt sind. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen zu speichern.

Tool zur Ereignissuche

Mit dem Tool zur Ereignissuche lassen sich einzelne Ereignisse rasch auffinden. So starten Sie die Suche nach einem bestimmten Ereignis:

1. Klicken Sie auf den Reiter **Events Browser** und wählen Sie den gewünschten Browser aus.

2. Wählen Sie im linken Fensterbereich unter **Actions** die Option **Find events**.



Screenshot 72 – Tool zur Ereignissuche

3. Geben Sie im oberen Bereich des Ereignisanzeige-Fensters die Suchparameter ein. Um bei der Suche die Groß-/Kleinschreibung zu beachten, klicken Sie in linken Fensterbereich auf **Options** und wählen Sie **Match case**.

4. Klicken Sie im oberen Bereich des Ereignisanzeige-Fensters auf die Schaltfläche **Find**, um die Suche zu starten.

Tool zum Export von Ereignissen

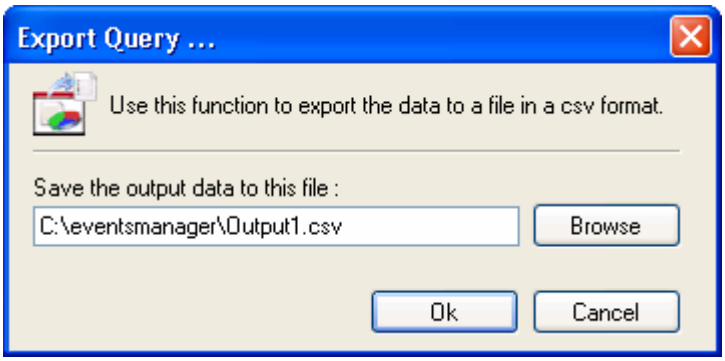
Ereignisdaten lassen sich direkt über die einzelnen Browser in CSV-Dateien exportieren, um weiterverarbeitet zu werden, z. B.

- zur Übermittlung von Informationen zu wichtigen Ereignissen per E-Mail,
- mithilfe automatisierter Skripten, die CSV-Daten in HTML-Inhalte für das Web/Firmen-Intranet konvertieren,
- zum Erstellen grafisch aufbereiteter Verwaltungsberichte und Statistiken mit Programmen wie Microsoft Excel,
- zum Anfertigen benutzerdefinierter Berichte in Drittanwendungen und
- zur Bereitstellung von Ereignisdaten für firmeninterne Anwendungen und Skripten

So exportieren Sie Ereignisse in CSV-Dateien:

1. Klicken Sie auf den Reiter **Events Browser** und wählen Sie den gewünschten Browser aus.

2. Wählen Sie die zu exportierenden Ereignisse aus. Klicken Sie mit der rechten Maustaste auf die Auswahl und wählen Sie im Kontextmenü **Export events**.


Export Query ...
Use this function to export the data to a file in a csv format.
Save the output data to this file :
C:\eventsmanager\Output1.csv
Browse
Ok
Cancel

Screenshot 73 – Tool zum Export von Ereignissen

3. Geben Sie den Speicherort für die Exportdatei an und klicken Sie auf die Schaltfläche **OK**.

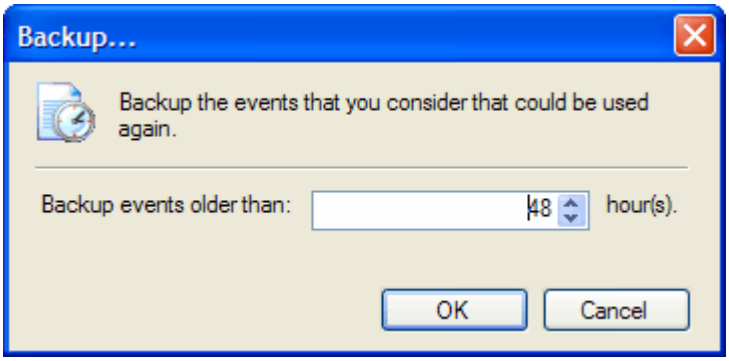
Sichern von Ereignissen

In der Hauptdatenbank gespeicherte Ereignisse lassen sich per Backup sichern. So verringern Sie die Größe der Datenbank und können weiterhin sämtliche Ereigniseinträge für forensische Sicherheitsanalysen und andere Kontrollen nutzen.

Mit der Funktion **Backup events** lassen sich alle Ereignisse sichern, die älter sind als von Ihnen angegeben. Die Zeitangabe erfolgt in Stunden. So werden Ereignisse gesichert:

1. Klicken Sie auf den Reiter **Events Browser** und wählen Sie den gewünschten Browser aus.

2. Wählen Sie im linken Fensterbereich unter **Actions** die Option **Backup events**.



Screenshot 74 – Backup von Ereignissen

3. Legen Sie fest, wie alt Ereignisse mindestens sein müssen (in Stunden), um gesichert zu werden. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen zu speichern.

Wechseln zwischen Datenbanken

Sie können zwischen der Haupt- und Backup-Datenbank wechseln, um Ereignisse in beiden Datenbanken anzuzeigen. Gehen Sie hierfür wie folgt vor:

1. Klicken Sie auf den Reiter **Events Browser** und wählen Sie den gewünschten Browser aus.

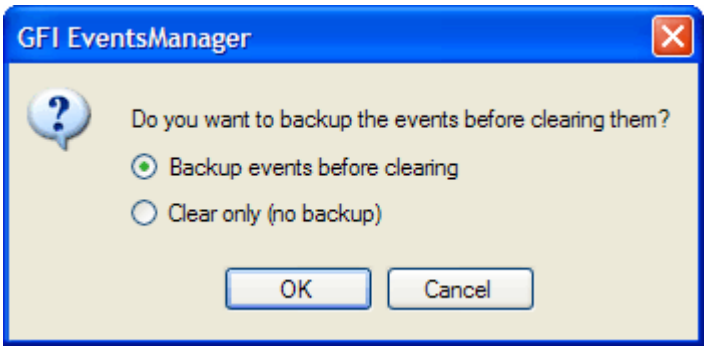
2. Wählen Sie im linken Fensterbereich unter **Common Tasks** die Option **Switch database**.

Löschen aller Ereignisse

So löschen Sie *alle* Ereignisse aus der aktuell ausgewählten Datenbank:

1. Klicken Sie auf den Reiter **Events Browser** und wählen Sie den gewünschten Browser aus.

2. Wählen Sie im linken Fensterbereich unter **Actions** die Option **Clear all events**.



Screenshot 75 – Löschen aller Ereignisse

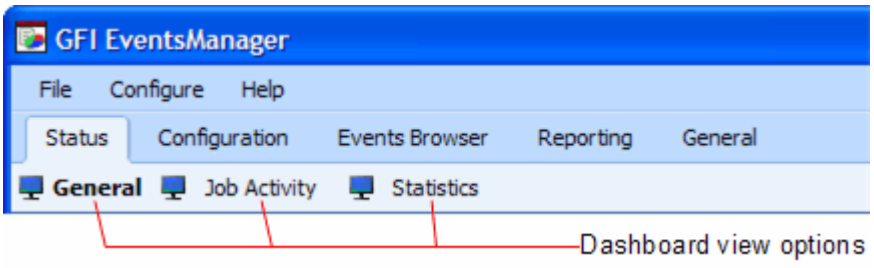
3. Haben Sie die Hauptdatenbank zur Anzeige von Ereignissen geöffnet, legen Sie fest, ob Ereignisse vor dem Löschen per Backup gesichert werden sollen (**Backup events before clearing**) oder einfach nur zu löschen sind (**Clear only (no backup)**).

Statusüberwachung

Einführung

Der Status-Monitor informiert über den aktuellen Programmstatus von GFI EventsManager und liefert statistische Informationen zu erfassten, verarbeiteten und archivierten Ereignissen. Es stehen hierfür drei unterschiedliche Ansichten zur Verfügung: **General** (Allgemein), **Job Activity** (Erfassungsabläufe) und **Statistics** (Statistiken).

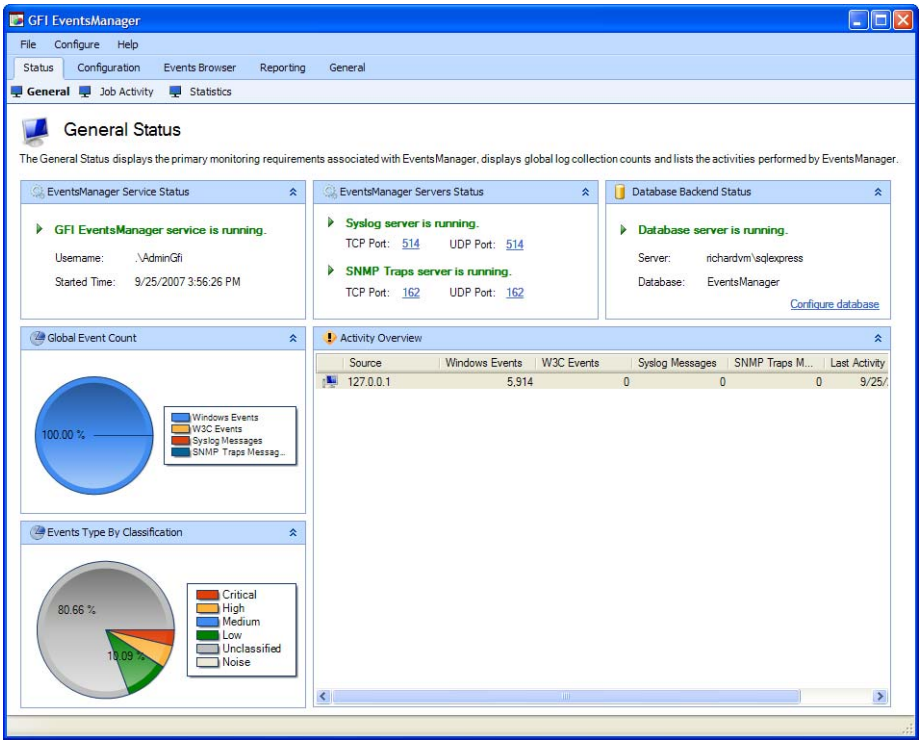
Aufrufen des Status-Monitors



Screenshot 76 – Anzeigeoptionen

Klicken Sie auf den Reiter **Status**, um den Status-Monitor aufzurufen. Wählen Sie die gewünschte Anzeigeoption aus. Weitere Informationen zu den jeweiligen Anzeigen erhalten Sie nachfolgend.

Ansicht zum allgemeinen Status („General“)



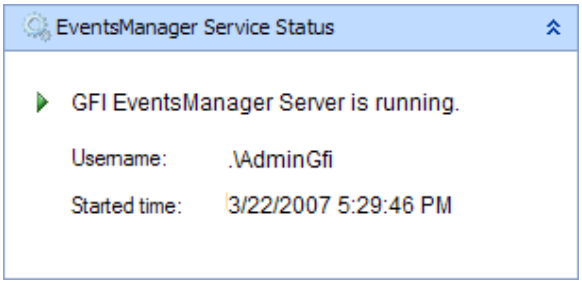
Screenshot 58 – Status von GFI EventsManager: Ansicht „General“

Folgende Informationen stehen über die Ansicht **General** bereit:

- Status der GFI EventsManager-Engine zur Ereignisverarbeitung
- Statistische Daten wie die Anzahl der pro Computer verarbeiteten Ereignisse

Die Informationen werden in einzelnen Bereichen angezeigt. Diese werden nachfolgend erläutert.

EventsManager Service Status



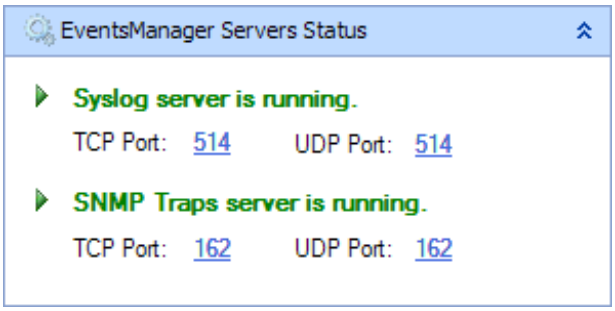
Screenshot 77 – Ansicht „General“: Dienststatus

Dieser Bereich informiert über:

- den Betriebsstatus der Ereignisverarbeitungs-Engine
- das Benutzerkonto, unter dem die GFI EventsManager-Engine läuft.
- den Startzeitpunkt der Ereignisverarbeitungs-Engine

Wichtiger Hinweis: Die Ereignisverarbeitungs-Engine bleibt deaktiviert, solange kein Datenbank-Backend eingerichtet ist.

EventsManager Servers Status

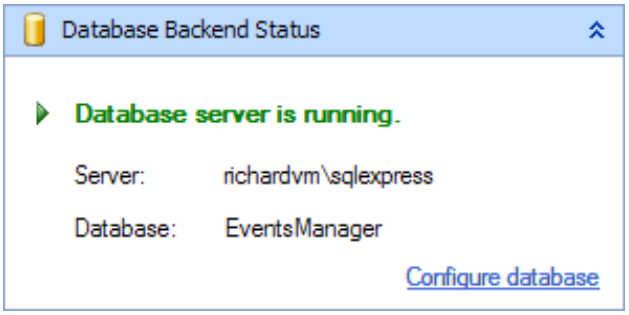

EventsManager Servers Status
Syslog server is running.
TCP Port: 514 UDP Port: 514
SNMP Traps server is running.
TCP Port: 162 UDP Port: 162

Screenshot 78 – Ansicht „General“: Server-Status

Dieser Bereich informiert über:

- den Betriebsstatus des Syslog-Servers
- die Port-Einstellung des Syslog-Servers
- den Betriebsstatus des SNMP-Trap-Servers
- die Port-Einstellung des SNMP-Trap-Servers

Database Backend Status

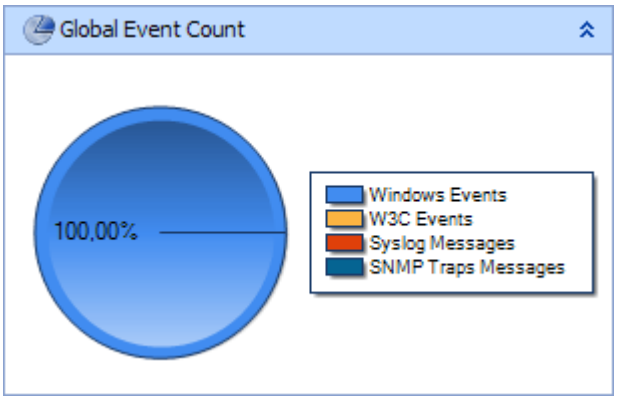


Screenshot 79 – Ansicht „General“: Status des Datenbank-Backends

Dieser Bereich informiert über:

- den Betriebsstatus des aktuell verwendeten Datenbank-Servers
- den Namen des aktuell verwendeten Datenbank-Servers
- den Namen der Datenbank, in der erfasste Ereignisse archiviert werden

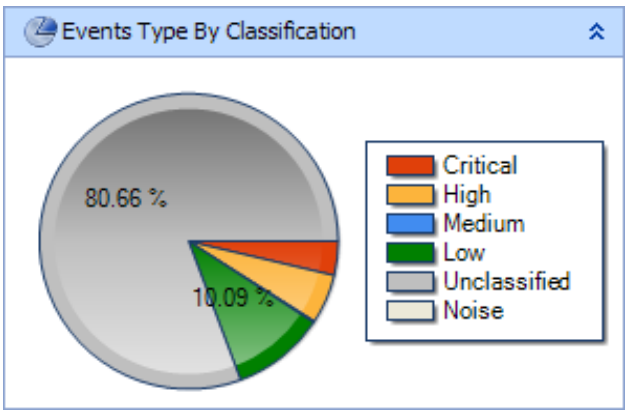
Global Event Count



Screenshot 80 – Ansicht „General“: Bereich „Global Event Count“

Dieser Bereich informiert anhand eines Kuchendiagramms über den prozentualen Anteil der von GFI EventsManager verarbeiteten Windows- und W3C-Ereignisse, Syslog-Meldungen und SNMP-Traps.

Events Type By Classification

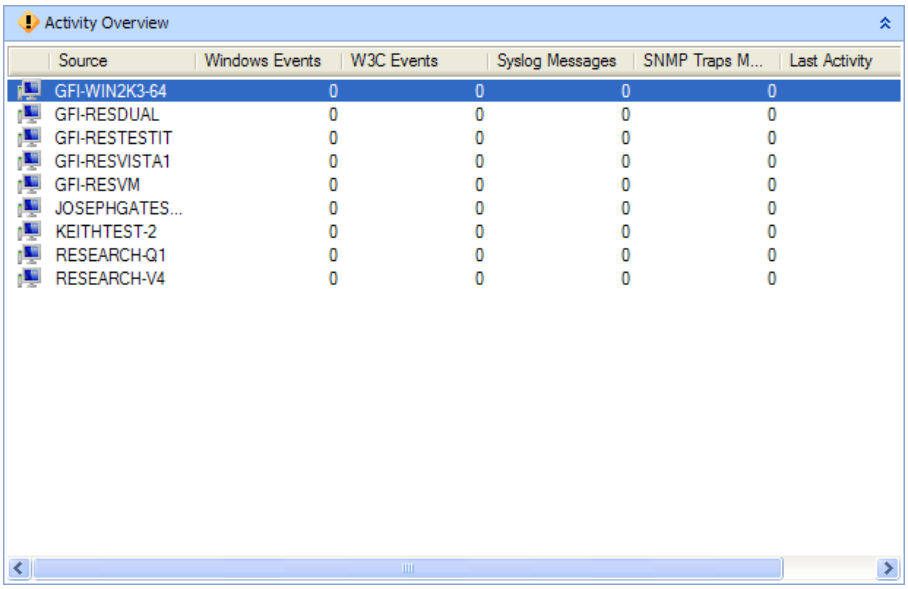


Screenshot 81 – Ansicht „General“: Bereich „Events Type By Classification“

Dieser Bereich informiert anhand eines Kuchendiagramms über den prozentualen Anteil von Ereignissen der Kategorien:

- Kritisch, hoch, mittel, niedrig
- Nicht klassifiziert

Activity Overview

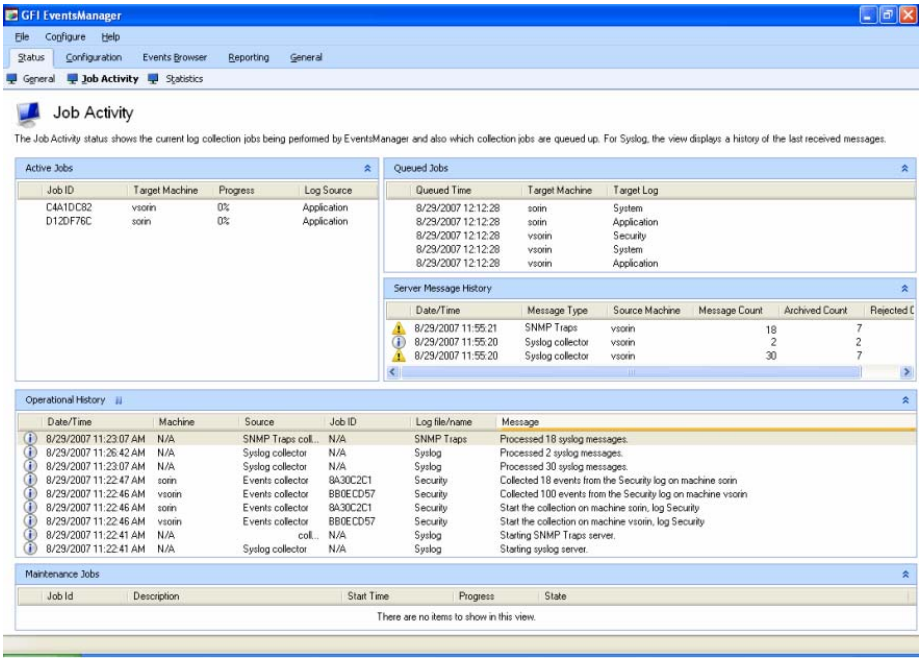


Screenshot 82 – Ansicht „General“: Bereich „Activity Overview“

Dieser Bereich informiert über:

- die Gesamtzahl der Windows- und W3C-Ereignisse, Syslog-Meldungen und SNMP-Traps je überwachten Computer
- das Datum des letzten von den jeweiligen Rechnern abgerufenen Ereignisses

Ansicht zu Erfassungsabläufen („Job Activity“)

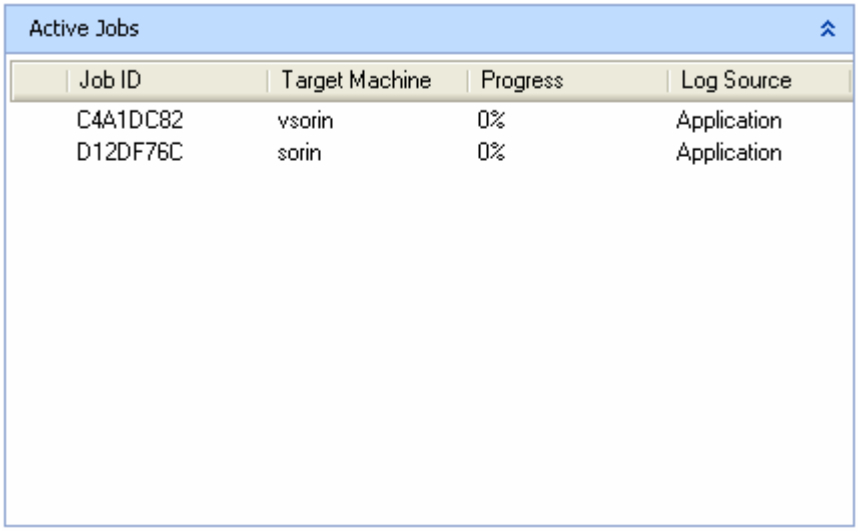

GFI EventsManager
File Configure Help
Status Configuration Events Browser Reporting General
General Job Activity Statistics
Job Activity
The Job Activity status shows the current log collection jobs being performed by EventsManager and also which collection jobs are queued up. For Syslog, the view displays a history of the last received messages.
Active Jobs
Job ID Target Machine Progress Log Source
C4A1DC82 vsorin 0% Application
D12DF76C sorin 0% Application
Queued Jobs
Queued Time Target Machine Target Log
8/29/2007 12:12:28 sorin System
8/29/2007 12:12:28 sorin Application
8/29/2007 12:12:28 vsorin Security
8/29/2007 12:12:28 vsorin System
8/29/2007 12:12:28 vsorin Application
Server Message History
Date/Time Message Type Source Machine Message Count Archived Count
8/29/2007 11:55:21 SNMP Traps vsorin 18 7
8/29/2007 11:55:20 Syslog collector vsorin 2 2
8/29/2007 11:55:20 Syslog collector vsorin 30 7
Operational History
Date/Time Machine Source Job ID Log file/name Message
8/29/2007 11:23:07 AM N/A SNMP Traps coll... N/A SNMP Traps Processed 18 syslog messages.
8/29/2007 11:26:42 AM N/A Syslog collector N/A Syslog Processed 2 syslog messages.
8/29/2007 11:23:07 AM N/A Syslog collector N/A Syslog Processed 30 syslog messages.
8/29/2007 11:22:47 AM sorin Events collector 8A30C2C1 Security Collected 18 events from the Security log on machine sorin
8/29/2007 11:22:46 AM vsorin Events collector BB0ECD57 Security Collected 100 events from the Security log on machine vsorin
8/29/2007 11:22:46 AM sorin Events collector 8A30C2C1 Security Start the collection on machine sorin, log Security
8/29/2007 11:22:46 AM vsorin Events collector BB0ECD57 Security Start the collection on machine vsorin, log Security
8/29/2007 11:22:41 AM N/A coll... N/A Syslog Starting SNMP Traps server.
8/29/2007 11:22:41 AM N/A Syslog collector N/A Syslog Starting syslog server.
Maintenance Jobs
Job Id Description Start Time Progress State
There are no items to show in this view.

Screenshot 83 - Status von GFI EventsManager: Ansicht „Job Activity“

Über die Ansicht **Job Activity** können Sie aktuelle Prozessabläufe kontrollieren, darunter die Ereigniserfassung und -verarbeitung. Für Syslog-Meldungen und SNMP-Traps steht ein separater Verlauf zur Verfügung.

Die Informationen werden in einzelnen Bereichen angezeigt. Diese werden nachfolgend erläutert.

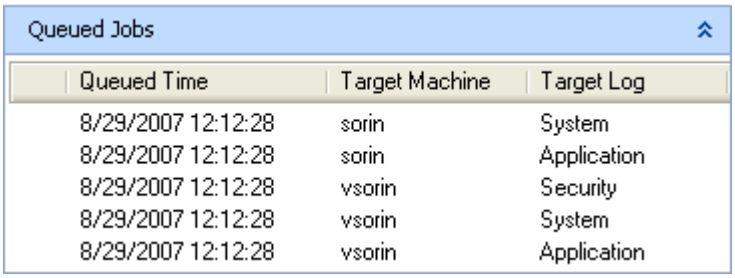
Active Jobs



Screenshot 84 – Ansicht „Job Activity“: Bereich „Active Jobs“

In diesem Bereich werden alle Erfassungsprozesse, die auf den überwachten Ereignisquellen aktiv sind, dargestellt. Zu den angezeigten Informationen zählen der aktuelle Erfassungsfortschritt in Prozent (**Progress**) und die Protokollquelle (**Log Source**).

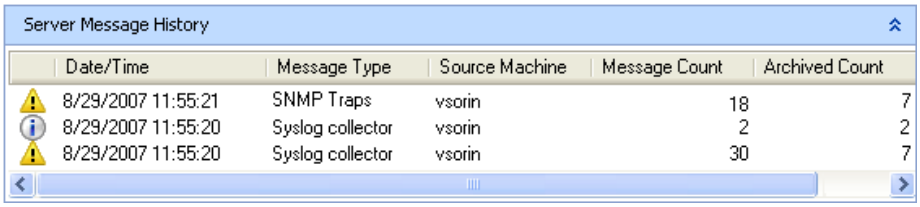
Queued Jobs



Screenshot 85 – Ansicht „Job Activity“: Bereich „Queued Jobs“

In diesem Bereich wird die Warteschlange aller noch ausstehenden Ereigniserfassungsvorgänge nach Computern aufgeschlüsselt dargestellt. Zu den angezeigten Informationen zählen die Protokollquelle, von der Ereignisse abgerufen werden sollen, und der Zeitpunkt, zu dem die Aufgabe in die Warteschlange gestellt wurde.

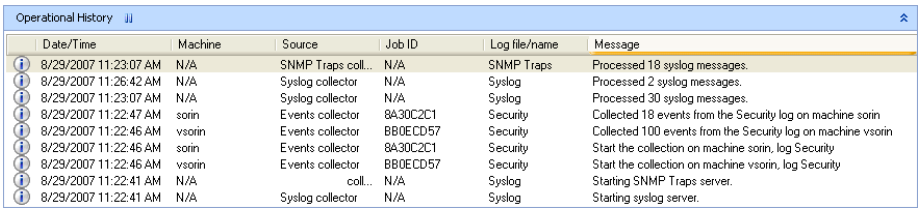
Server Message History



Screenshot 86 – Ansicht „Job Activity“: Bereich „Server Message History“

In diesem Bereich werden alle Server-Meldungen (SNMP-Traps und Syslog) dargestellt, die von GFI EventsManager empfangen wurden. Zu den angezeigten Informationen zählen die Gesamtzahl der von jeder Ereignisquelle verschickten Meldungen und der Zeitpunkt, zu dem die letzte Meldung empfangen wurde.

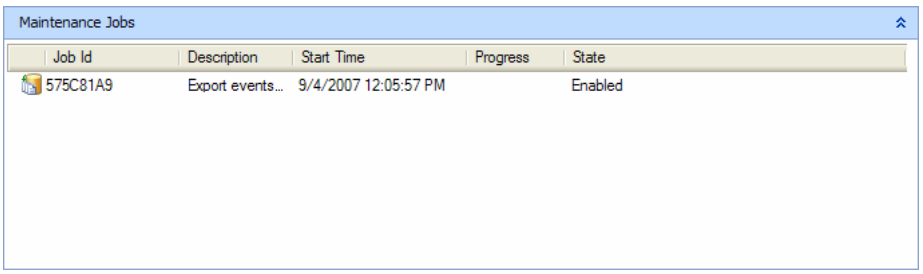
Operational History


Operational History
Date/Time
Machine
Source
Job ID
Log file/name
Message
8/29/2007 11:23:07 AM N/A SNMP Traps coll... N/A SNMP Traps Processed 18 syslog messages.
8/29/2007 11:26:42 AM N/A Syslog collector N/A Syslog Processed 2 syslog messages.
8/29/2007 11:23:07 AM N/A Syslog collector N/A Syslog Processed 30 syslog messages.
8/29/2007 11:22:47 AM sorin Events collector 8A30C2C1 Security Collected 18 events from the Security log on machine sorin
8/29/2007 11:22:46 AM vsorin Events collector BB0ECD57 Security Collected 100 events from the Security log on machine vsorin
8/29/2007 11:22:46 AM sorin Events collector 8A30C2C1 Security Start the collection on machine sorin, log Security
8/29/2007 11:22:46 AM vsorin Events collector BB0ECD57 Security Start the collection on machine vsorin, log Security
8/29/2007 11:22:41 AM N/A coll... N/A Syslog Starting SNMP Traps server.
8/29/2007 11:22:41 AM N/A Syslog collector N/A Syslog Starting syslog server.

Screenshot 87 – Ansicht „Job Activity“: Bereich „Operational History“

In diesem Bereich sind alle von GFI EventsManager durchgeführten Aktionen zur Ereigniserfassung chronologisch aufgeführt. Angezeigt werden während der Erfassung ausgegebene Fehlermeldungen und andere Informationen sowie der Name der auf dem Zielrechner überprüften Protokolldatei.

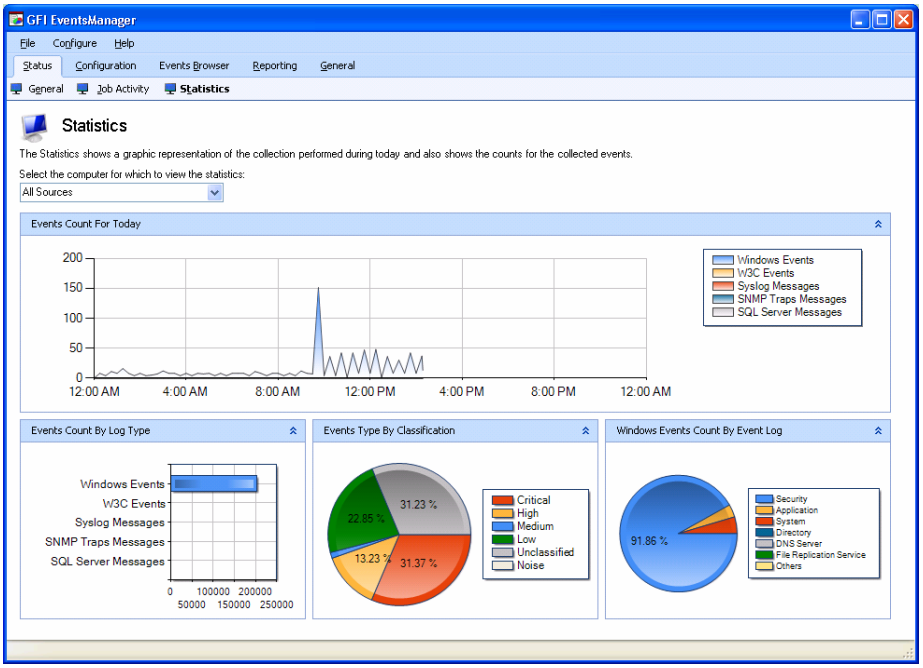
Maintenance Jobs



Screenshot 88 – Ansicht „Job Activity“: Bereich „Maintenance Jobs“

In diesem Bereich wird der Fortschritt von Wartungsaufgaben angezeigt, die über die **Database Operations** (Datenbank-operationen) festgelegt wurden. Angezeigt werden zudem die Beschreibung der einzelnen Aufgaben und deren Startzeitpunkt.

Ansicht zu Statistiken („Statistics“)

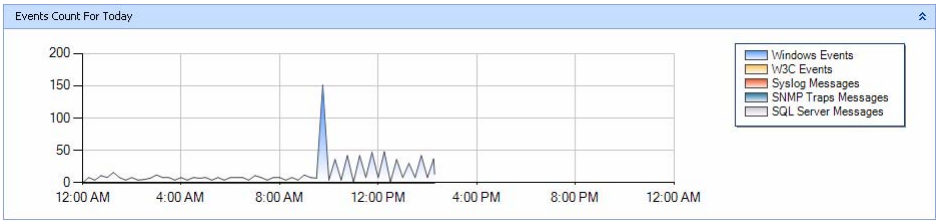


Screenshot 89 – Ansicht „Statistics“

Über die Ansicht **Statistics** können Sie Trends bei täglichen Ereignissen feststellen und Statistikinformationen zu einzelnen Computern Ihres Netzwerks abrufen.

Die Informationen werden in einzelnen Bereichen angezeigt. Diese werden nachfolgend erläutert.

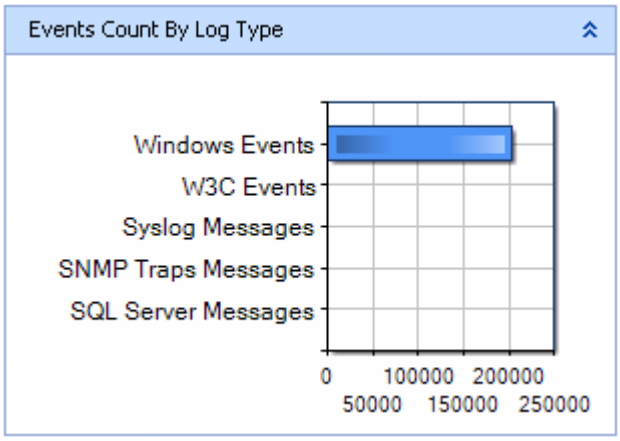
Events Count For Today



Screenshot 90 – Ansicht „Statistics“: Bereich „Events Count For Today“

In diesem Bereich werden rechner- und netzwerkspezifische Ereignistrends im Tagesablauf anhand eines Kurvendiagramms angezeigt. Dabei erfolgt eine farbliche Unterscheidung zwischen Windows- und W3C-Ereignissen, Syslog-Meldungen und SNMP-Traps.

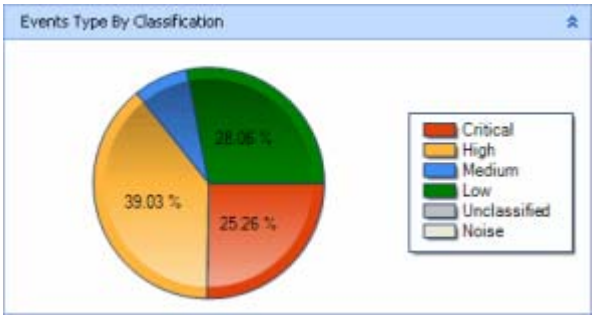
Events Count By Log Type



Screenshot 91 – Ansicht „Statistics“: Bereich „Events Count By Log Type“

In diesem Fenster wird die Anzahl aller für einen Rechner oder ein Netzwerk erfassten Windows- und W3C-Ereignisse, Syslog- und SQL-Server-Meldungen und SNMP-Traps anhand eines Balkendiagramms angezeigt.

Events Type By Classification

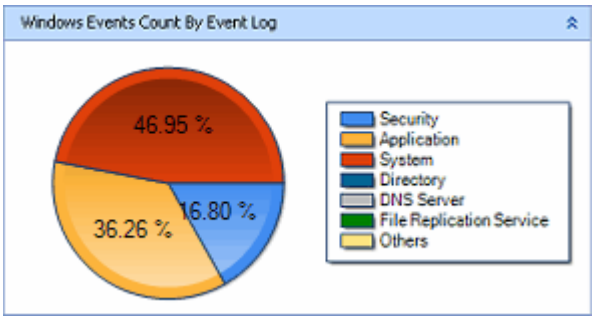


Screenshot 92 – Ansicht „Statistics“: Bereich „Events Count by Classification“

In diesem Bereich werden anhand eines Kuchendiagramms rechner- oder netzwerkspezifische Ereignisse folgender Kategorien prozentual dargestellt:

- Kritisch, hoch, mittel, niedrig
- Nicht klassifiziert

Windows Events Count By Event Log



Screenshot 93 – Ansicht „Statistics“: Bereich „Windows Events Count by Event Log“

In diesem Fenster wird anhand eines Kuchendiagramms der prozentuale Anteil der Windows-Ereignisse aus den Protokollen Sicherheit, System, Anwendungen, DNS-Server, Verzeichnisse und Dateireplikation und Andere angezeigt.

Datenbankoperationen

Einführung

Das Modul **Database Operations** von GFI EventsManager unterstützt Administratoren bei folgenden Aufgaben der Datenbankwartung:

- Zusammenführung von Ereignissen, die entfernte GFI EventsManager-Instanzen erfasst haben, in einem zentralen Datenbank-Backend
- Optimierung der Leistung von GFI EventsManager durch aktives Überwachen der Größe des Datenbank-Backends
- Import und Export von Daten in/von GFI EventsManager-Installationen der Version 8.x ohne Dateninkonsistenz

Gründe für die Datenbankwartung

Die Datenbank muss regelmäßig gewartet werden, um einen übermäßig großen Datenbestand zu vermeiden. Die Leistung von GFI EventsManager wird bei Verwendung einer zu umfassenden Datenbank bedeutend eingeschränkt: Ereignisse lassen sich nur mit Verzögerung durchsuchen, und Abfragen werden verlangsamt. Auch die Berichterstellung mit dem Reporting-Modul GFI EventsManager ReportPack beansprucht mehr Zeit.

Die Leistung des Datenbank-Backends lässt sich über die **Database Operations** optimieren. Es stehen mehrere Optionen für Wartungsaufgaben bereit. Hierzu zählen:

- **Move to database** – Mit diesem Vorgang werden Ereignisse aus der Haupt-Datenbank in die Backup- oder eine andere Datenbank verschoben.
- **Export to file** – Mit diesem Vorgang werden Ereignisse aus der Haupt-Datenbank in eine komprimierte Binärdatei exportiert. Diese lässt sich verschlüsseln und auf CD/DVD oder einem anderen Datenträger sichern.
- **Import from file** – Mit diesem Vorgang lassen sich Ereignisse aus Exportdateien von GFI EventsManager in die Haupt-Datenbank importieren.
- **Delete data** – Mit diesem Vorgang lassen sich Ereignisse aus dem Haupt- oder Backup-Datenbank-Backend löschen.

Für alle Vorgänge lassen sich zudem Filter zur gezielteren Wartung einrichten.

Konsolidieren von Ereignissen in einem WAN

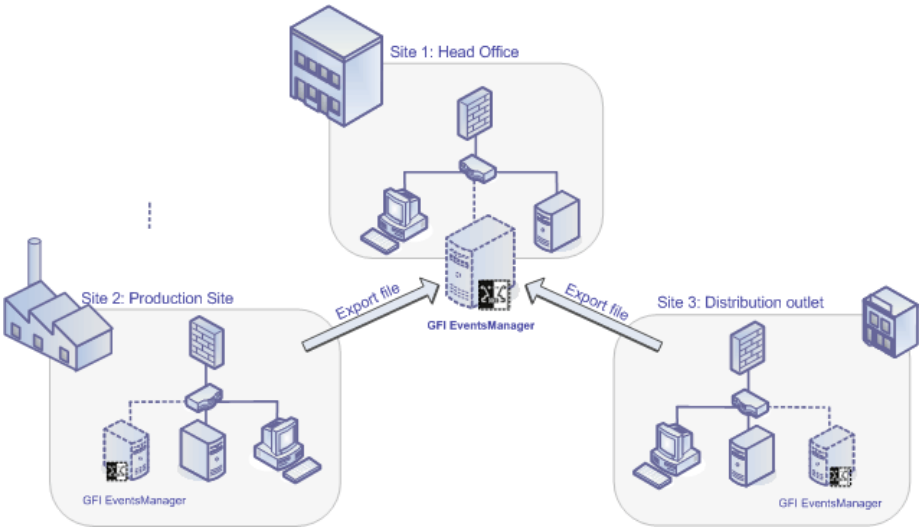


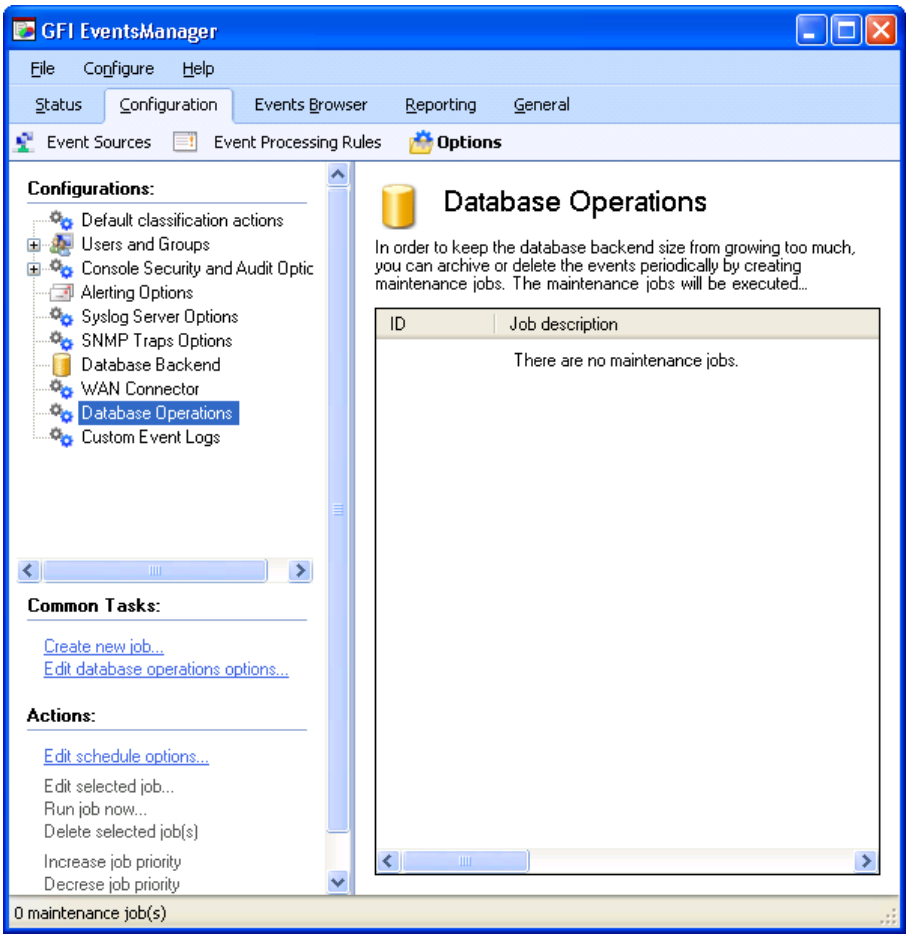
Abbildung 1: Konsolidieren von Ereignissen in einem WAN

Bei Unternehmen mit mehreren Niederlassungen können einzelne oder alle erfassten Ereignisdaten der verteilten Dependancen mit den **Database Operations** in einer zentralen Datenbank konsolidiert werden. Zunächst werden die Daten per **Export to file** vorbereitet, d. h. in einer Datei komprimiert und verschlüsselt, und dann zur zentralen Verarbeitung exportiert. Nach dem Empfang werden sie per **Import to file** in die zentrale Datenbank importiert.

Der **Events Browser** erlaubt später die Anzeige der von den entfernten Standorten erfassten Ereignisse. Die in dieser Form in der zentralen Datenbank gesicherten Ereignisse lassen sich zudem zum Erstellen niederlassungsspezifischer Ereignisberichte nutzen.

Konfigurieren der Datenbankwartung per Database Operations

Legen Sie fest, wann Wartungsarbeiten erfolgen sollen (Uhrzeit und Tag sowie Wartungsintervalle).



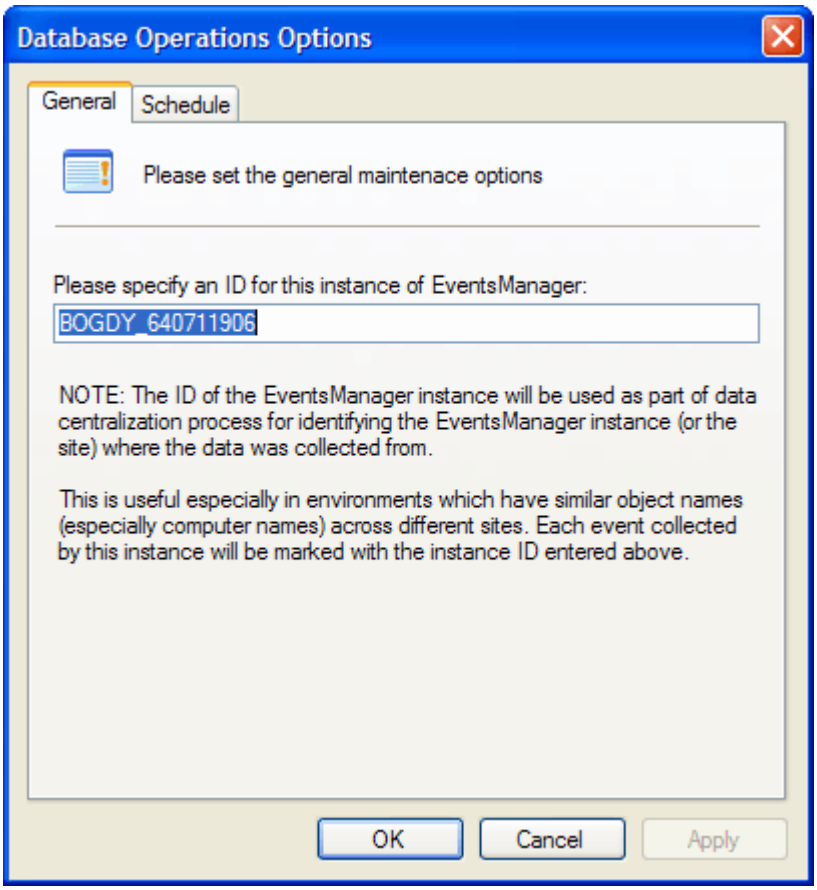
Screenshot 94 – Konfigurierung der Database Operations

Hinweis: Die Datenbankwartung kann zu Lasten der Leistung des Servers und von GFI EventsManager gehen. Für eine uneingeschränkte Verfügbarkeit Ihrer Systemressourcen und zur Vermeidung von Beeinträchtigungen sollten diese Arbeiten daher außerhalb der normalen Geschäftszeiten erfolgen.

So konfigurieren Sie die **Database Operations**:

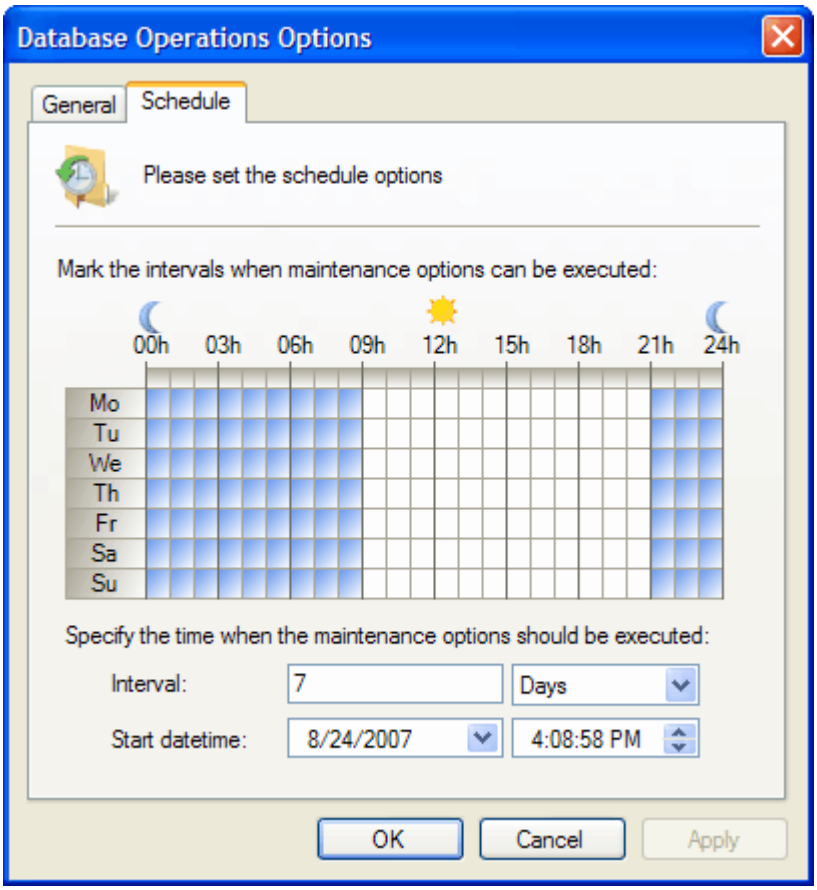
1. Klicken Sie auf den Reiter **Configuration** ▸ **Options**.

2. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf den Knoten **Database Operations** und wählen Sie im Kontextmenü **Properties**.


Database Operations Options
General
Schedule
Please set the general maintenace options
Please specify an ID for this instance of EventsManager:
BOGDY_640711906
NOTE: The ID of the EventsManager instance will be used as part of data centralization process for identifying the EventsManager instance (or the site) where the data was collected from.
This is useful especially in environments which have similar object names (especially computer names) across different sites. Each event collected by this instance will be marked with the instance ID entered above.
OK
Cancel
Apply

Screenshot 95 – Optionen zur Datenbankwartung: Eindeutige Kennung einer Instanz von GFI EventsManager

3. Geben Sie der jeweiligen Instanz von GFI EventsManager eine eindeutige Kennung, die der Identifizierung im Netzwerk dient. Diese ID ist bei dem Vorgang **Export to file** Bestandteil des Namens der zu exportierenden Datei.



Screenshot 96 – Optionen zur Datenbankwartung: Wartung nach Zeitplan

4. Klicken Sie auf den Reiter **Schedule**, um folgende Einstellungen festzulegen:

- Tageszeiten, zu denen Wartungsarbeiten durchgeführt werden können.
- Der Zeitabstand (in Stunden/Tagen), in dem Wartungsarbeiten erfolgen sollen.
- Der Startzeitpunkt für die erste Durchführung von Wartungsarbeiten.

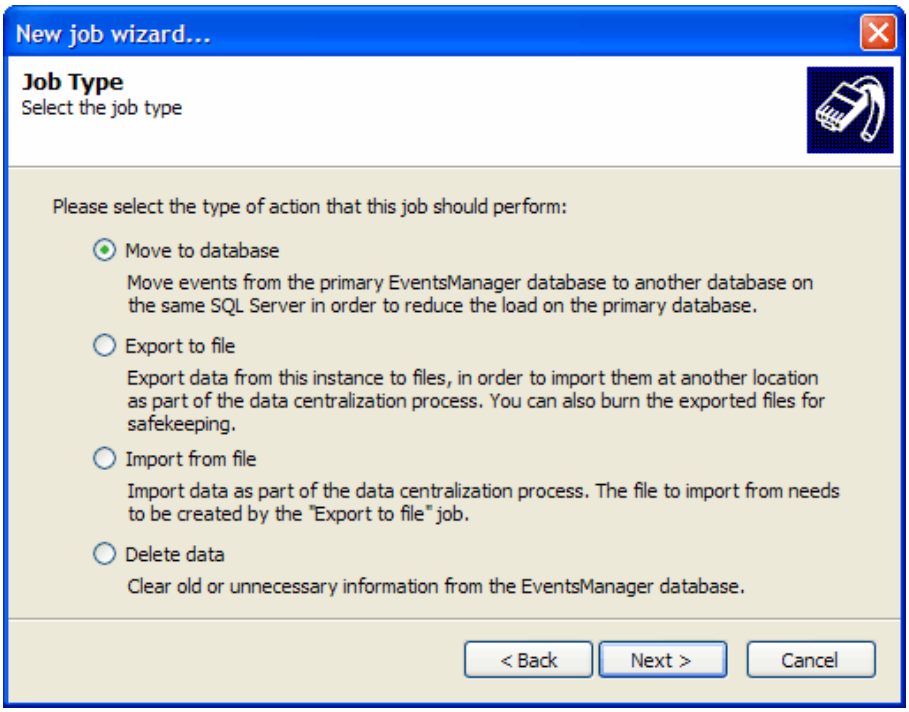
Einrichten einer Wartungsaufgabe

So richten Sie eine neue Wartungsaufgabe ein:

1. Klicken Sie auf den Reiter **Configuration** ▸ **Options**.

2. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf den Knoten **Database Operations** und wählen Sie **Create new job…** Der Assistent zum Einrichten neuer Wartungsaufgaben („New job wizard“) wird aufgerufen.

3. Klicken Sie auf die Schaltfläche **Next**, um zum Auswahlschritt **Job Type** zu gelangen.

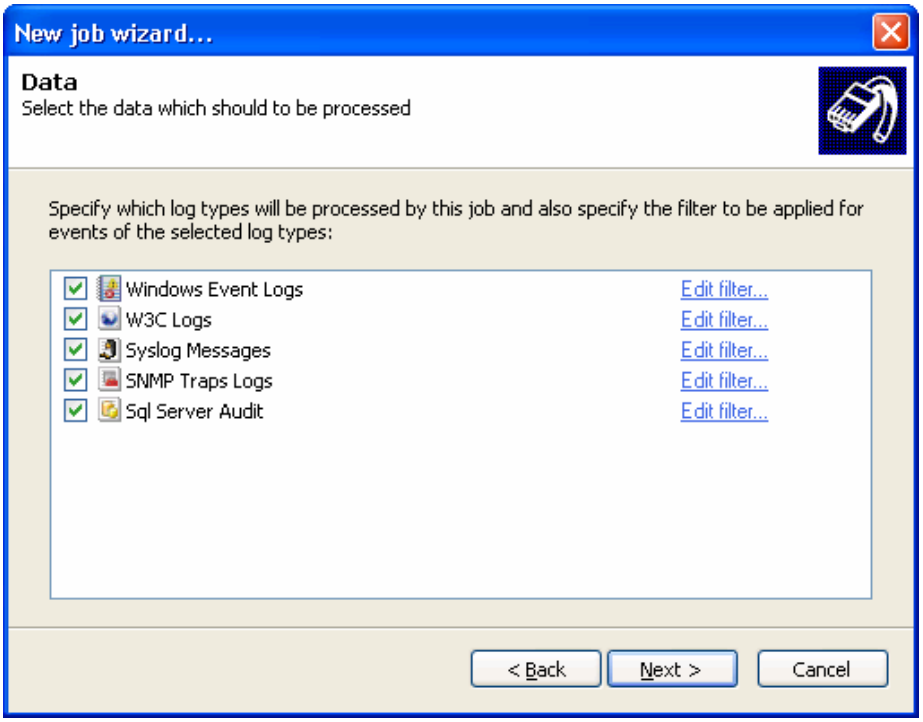

New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Move to database
Move events from the primary EventsManager database to another database on the same SQL Server in order to reduce the load on the primary database.
Export to file
Export data from this instance to files, in order to import them at another location as part of the data centralization process. You can also burn the exported files for safekeeping.
Import from file
Import data as part of the data centralization process. The file to import from needs to be created by the "Export to file" job.
Delete data
Clear old or unnecessary information from the EventsManager database.
< Back
Next >
Cancel

Screenshot 97 – Assistent zum Einrichten einer neuen Wartungsaufgabe: Auswahl des Aufgabentyps

4. Wählen Sie den gewünschten Aufgabentyp aus.

5. Geben Sie alle erforderlichen Parameter an und klicken Sie auf die Schaltfläche **Next**.

Hinweis: Weitere Informationen zur Festlegung der Parameter einer einzelnen Wartungsaufgabe erhalten Sie weiter unten in diesem Kapitel.


New job wizard...
Data
Select the data which should to be processed
Specify which log types will be processed by this job and also specify the filter to be applied for events of the selected log types:
Windows Event Logs
Edit filter...
W3C Logs
Edit filter...
Syslog Messages
Edit filter...
SNMP Traps Logs
Edit filter...
Sql Server Audit
Edit filter...
< Back
Next >
Cancel

Screenshot 98 – Datenfilterung mit Angabe einzelner Filterbedingungen

6. Wählen Sie aus, welche Ereignisprotokolle verarbeitet werden sollen. Legen Sie zudem per Klick auf **Edit filter** fest, welche Daten der jeweiligen Protokolle aus dem Datenbank-Backend herausgefiltert werden sollen. Wird kein Filter angegeben, werden mit der ausgewählten Wartungsaufgabe aller Daten des Datenbank-Backends bearbeitet. Klicken Sie auf die Schaltfläche **Next**.

Hinweis: Weitere Informationen zur Festlegung von Filter-bedingungen erhalten Sie unter „Konfigurieren der Datenfilter-Bedingungen" in diesem Kapitel.

New job wizard...
Completing the "New Job" Wizard
Select when the job should be executed:
Scheduled job
The job will be saved and executed according to the Enterprise Maintenance schedule options.
Run the job now
The job will be executed only once.
GFI
< Back
Finish
Cancel

Screenshot 99 – Zeitpunkt der Durchführung der Wartungsaufgabe

7. Legen Sie fest, ob die Wartungsaufgabe nach Zeitplan oder sofort und nur einmalig durchzuführen ist.

Hinweis 1: Aufgaben nach Zeitplan werden gemäß den Vorgaben der **Database Operations** durchgeführt.

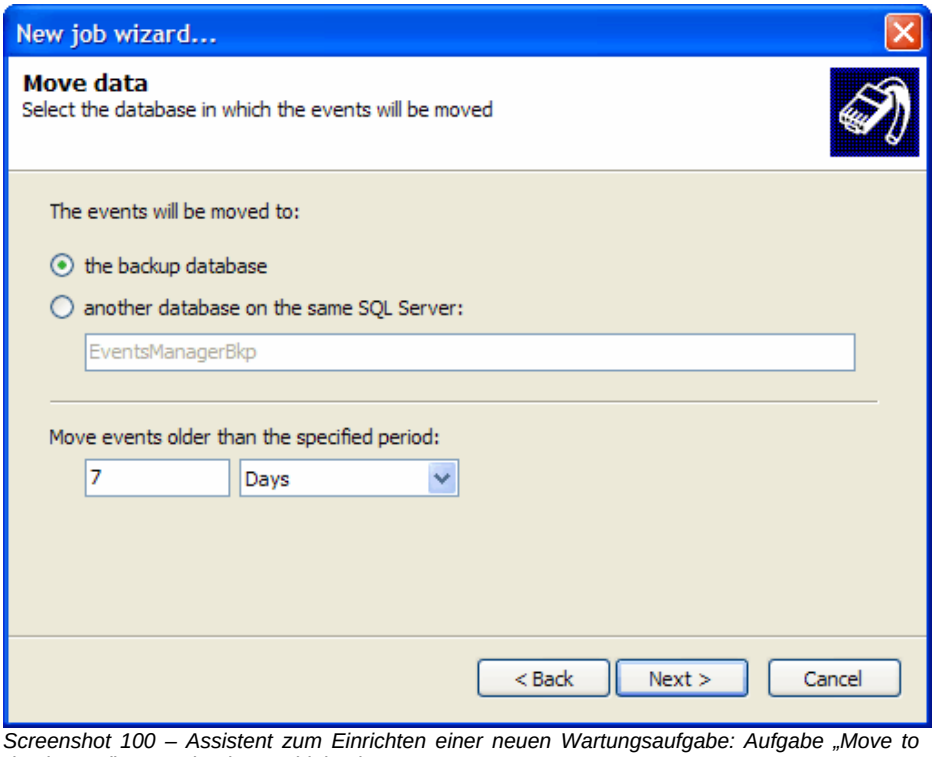
Hinweis 2: Andere ausgewählte Wartungsaufgaben werden nur einmal durchgeführt.

8. Klicken Sie auf die Schaltfläche **Finish**, um die Konfigurierung abzuschließen.

Aufgabe „Move to database“ (in Datenbank verschieben)

So erstellen Sie eine Wartungsaufgabe, mit der Ereignisse aus der Haupt-Datenbank in eine andere Datenbank verschoben werden:

1. Starten Sie den Assistenten für neue Wartungsaufgaben, wie oben unter „Einrichten einer Wartungsaufgabe“ beschrieben, und wählen Sie die Aufgabe **Move to database**.



Screenshot 100 – Assistent zum Einrichten einer neuen Wartungsaufgabe: Aufgabe „Move to database“ (in Datenbank verschieben)

2. Geben Sie die Datenbank an, in die Ereignisse verschoben werden sollen. Hierbei sollte es sich um die Backup-Datenbank handeln oder um eine andere zugängliche Datenbank auf dem SQL-Server mit der Haupt-Datenbank.

3. Legen Sie mit der Option **Move events older than the specified period** fest, dass nur vor dem angegebenen Zeitraum eingetretene Ereignisse verschoben werden.

4. Klicken Sie auf die Schaltfläche **Next**.

5. Legen Sie weitere Filterbedingungen für diese Aufgabe fest. Andernfalls werden alle Ereignisse, die älter sind als von Ihnen festgelegt, verschoben. Klicken Sie auf die Schaltfläche **Next**.

Hinweis: Weitere Informationen zur Festlegung von Filter-bedingungen erhalten Sie unter „Konfigurieren der Datenfilter-Bedingungen" in diesem Kapitel.

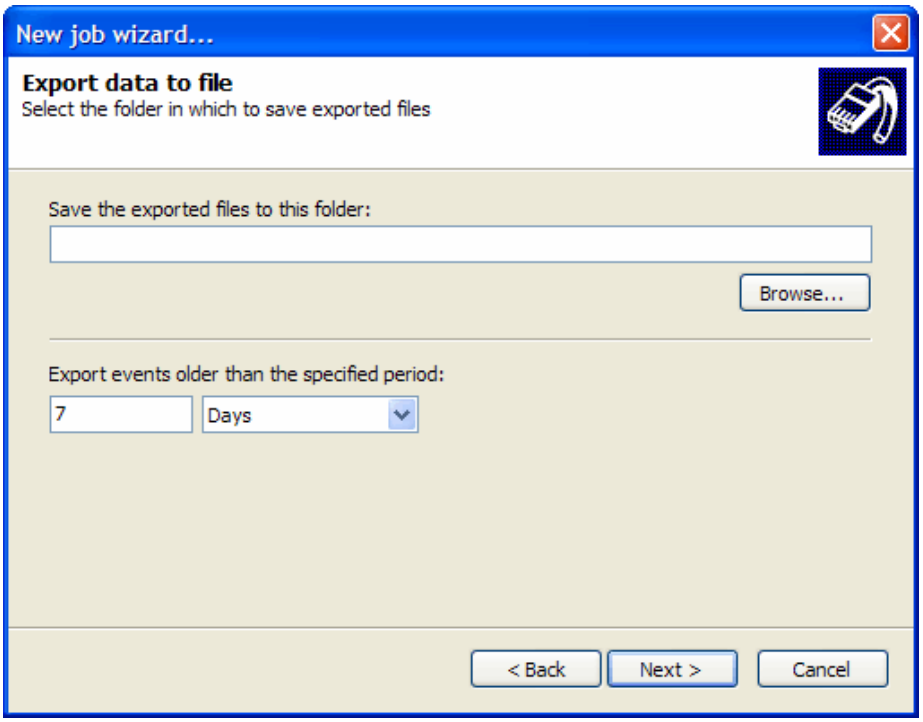
6. Legen Sie fest, ob die Wartungsaufgabe nach Zeitplan oder sofort und nur einmalig durchzuführen ist.

7. Klicken Sie auf die Schaltfläche **Finish**, um die Konfigurierung der Wartungsaufgabe zu beenden.

Aufgabe „Export to file“ (in Datei exportieren)

So exportieren Sie Ereignisse aus der Haupt-Datenbank in eine Binärdatei:

1. Starten Sie den Assistenten für neue Wartungsaufgaben, wie oben unter „Einrichten einer Wartungsaufgabe“ beschrieben, und wählen Sie die Aufgabe **Export to file**.



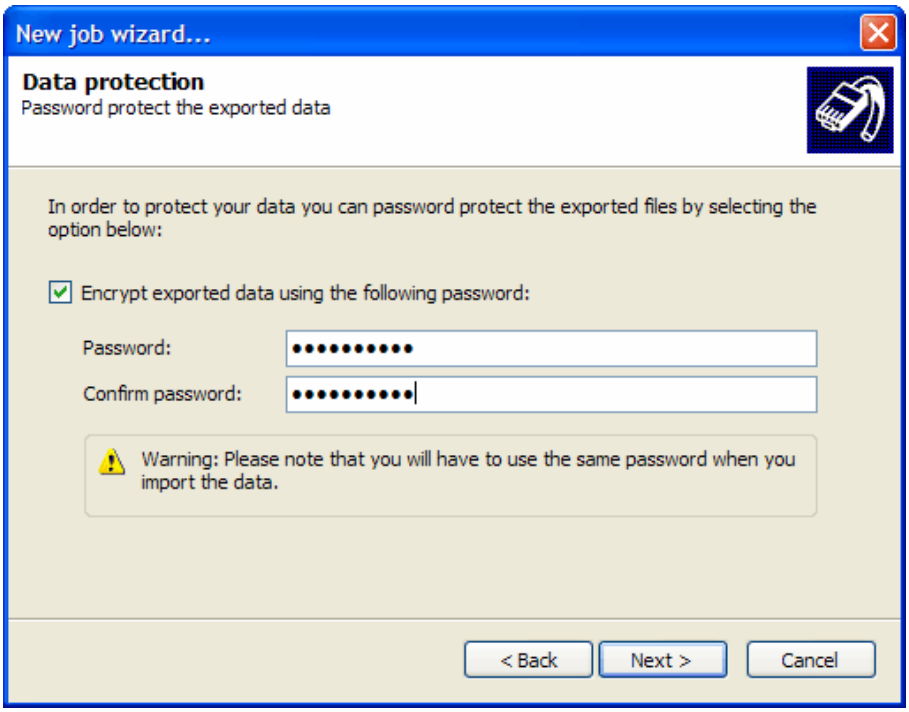
Screenshot 101 – Assistent zum Einrichten einer neuen Wartungsaufgabe: Aufgabe „Export to file“ (in Datei exportieren)

2. Geben Sie den Zielordner für die Exportdatei an. Verwenden Sie für Speicherpfade entfernter Ziele die UNC-Syntax.

Hinweis: Stellen Sie sicher, dass GFI EventsManager administrative Zugriffsrechte auf den Zielordner besitzt.

3. Legen Sie mit der Option **Export events older than the specified period** fest, dass nur vor dem angegebenen Zeitraum eingetretene Ereignisse exportiert werden.

4. Klicken Sie auf die Schaltfläche **Next**, um ein Passwort zum Schutz der Exportdaten einzurichten.


New job wizard...
Data protection
Password protect the exported data
In order to protect your data you can password protect the exported files by selecting the option below:
Encrypt exported data using the following password:
Password:
Confirm password:
Warning: Please note that you will have to use the same password when you import the data.
< Back
Next >
Cancel

Screenshot 102 – Assistent zum Einrichten einer neuen Wartungsaufgabe: Passwortschutz für eine Exportdatei

5. Wählen Sie durch Markieren der Option **Encrypt exported data using the following password** aus, ob die zu exportierenden Ereignisdaten mit einem Passwort verschlüsselt werden sollen, und geben Sie dieses ggf. an. Klicken Sie auf die Schaltfläche **Next**, um weitere Filterbedingungen für Ereignisdaten zu definieren.

Hinweis 1: Wählen Sie ein sicheres Passwort zur Verschlüsselung aus. Beachten Sie, dass dieses zum Import der Datei erneut verwendet werden muss.

6. Legen Sie weitere Filterbedingungen für diese Aufgabe fest. Andernfalls werden alle Ereignisse, die älter sind als von Ihnen festgelegt, exportiert. Klicken Sie auf die Schaltfläche **Next**.

Hinweis: Weitere Informationen zur Festlegung von Filterbedingungen erhalten Sie unter „Konfigurieren der Datenfilter-Bedingungen" in diesem Kapitel.

7. Legen Sie fest, ob die Wartungsaufgabe nach Zeitplan oder sofort und nur einmalig durchzuführen ist.

8. Klicken Sie auf die Schaltfläche **Finish**, um die Konfigurierung abzuschließen.

Benennung der Exportdatei

Exportdateien werden von GFI EventsManager nach folgendem Schema benannt:

[ESM-ID]_[Aufgaben-ID]_[Datum von]_[Datum bis].EXP

- *ESM-ID* – Zeigt die eindeutige Kennung der zugehörigen Instanz von GFI EventsManager an.
- *Aufgaben-ID* – Zeigt die eindeutige Kennung der Wartungsaufgabe an.

- *Datum von* – Informiert über das Datum des am längsten zurückliegenden Ereignisses, das exportiert wurde.
- *Datum bis* – Informiert über das Datum des neuesten Ereignisses, das exportiert wurde.
- *.EXP* – Bezeichnet die Dateierweiterung aller Exportdateien.

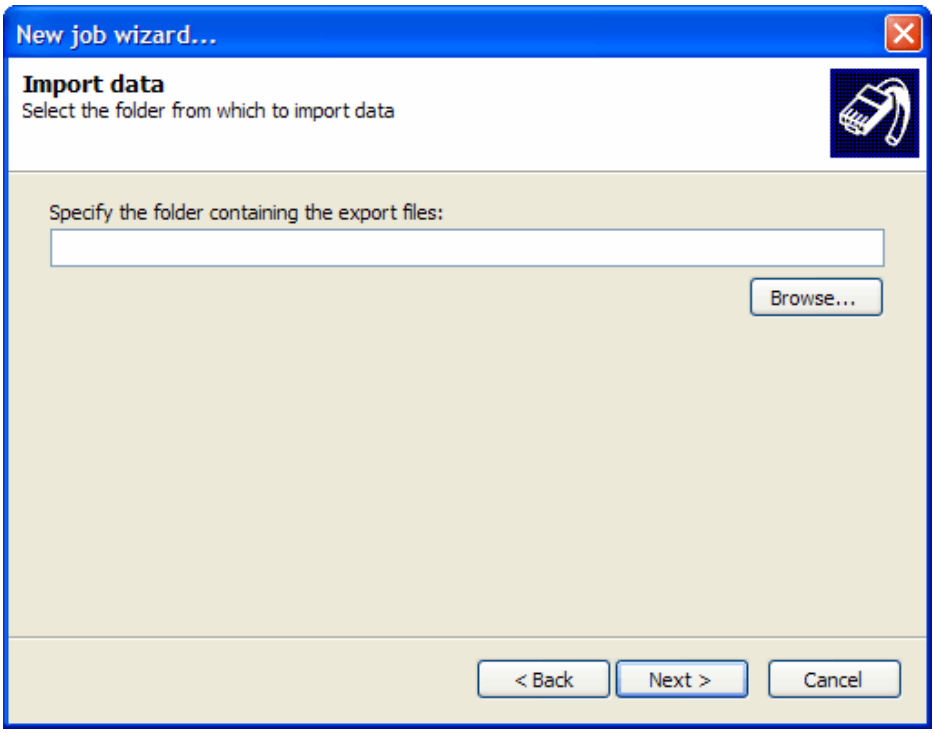
Folgendes Beispiel zeigt den Namen einer Exportdatei:

SERVER01_0051_20061020_20061025.EXP

Aufgabe „Import from file“ (aus Datei importieren)

So importieren Sie in einer Exportdatei gesicherte Ereignisse in die Haupt-Datenbank:

1. Starten Sie den Assistenten für neue Wartungsaufgaben, wie oben unter „Einrichten einer Wartungsaufgabe“ beschrieben, und wählen Sie die Aufgabe **Import from file**.



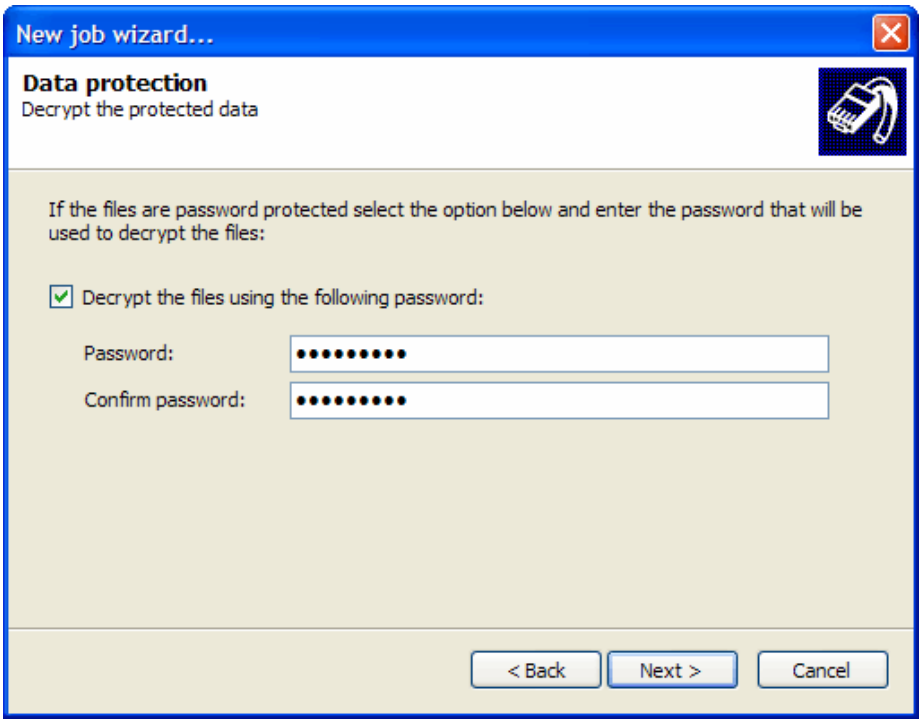
Screenshot 103 – Assistent zum Einrichten einer neuen Wartungsaufgabe: Aufgabe „Import from file“ (aus Datei importieren)

2. Geben Sie den Speicherort der Exportdatei an. Verwenden Sie für Speicherpfade entfernter Ziele die UNC-Syntax.

Hinweis 1: Stellen Sie sicher, dass GFI EventsManager administrative Zugriffsrechte auf den Ordner besitzt, in dem sich die Datei befindet.

Hinweis 2: GFI EventsManager importiert alle Dateien mit der Erweiterung .EXP.

3. Klicken Sie auf die Schaltfläche **Next**, um das Passwort zur Freigabe der Exportdaten anzugeben.


New job wizard...
Data protection
Decrypt the protected data
If the files are password protected select the option below and enter the password that will be used to decrypt the files:
Decrypt the files using the following password:
Password:
Confirm password:
< Back
Next >
Cancel

Screenshot 104 – Assistent zum Einrichten einer neuen Wartungsaufgabe: Angabe des Passworts bei der Aufgabe „Import from file“

4. Geben Sie das Passwort zur Freigabe der Ereignisdaten an. Klicken Sie auf die Schaltfläche **Next**, um Filter für die Ereignisdaten zu definieren.

Hinweis: Verwenden Sie das Passwort, das zur Verschlüsslung der Ereignisdaten verwendet wurde.

5. Definieren Sie Filter, die auf die importierte Datei angewendet werden sollen. Klicken Sie auf die Schaltfläche **Next**.

Hinweis 1: Mit Hilfe der für zu importierende Dateien definierbaren Filter lassen sich Ereignisse gezielt in die Haupt-Datenbank importieren.

Hinweis 2: Weitere Informationen zur Festlegung von Filterbedingungen erhalten Sie unter „Konfigurieren der Filterbedingungen" in diesem Kapitel.

6. Legen Sie fest, ob die Wartungsaufgabe nach Zeitplan oder sofort und nur einmalig durchzuführen ist.

7. Klicken Sie auf die Schaltfläche **Finish**, um die Konfigurierung abzuschließen.

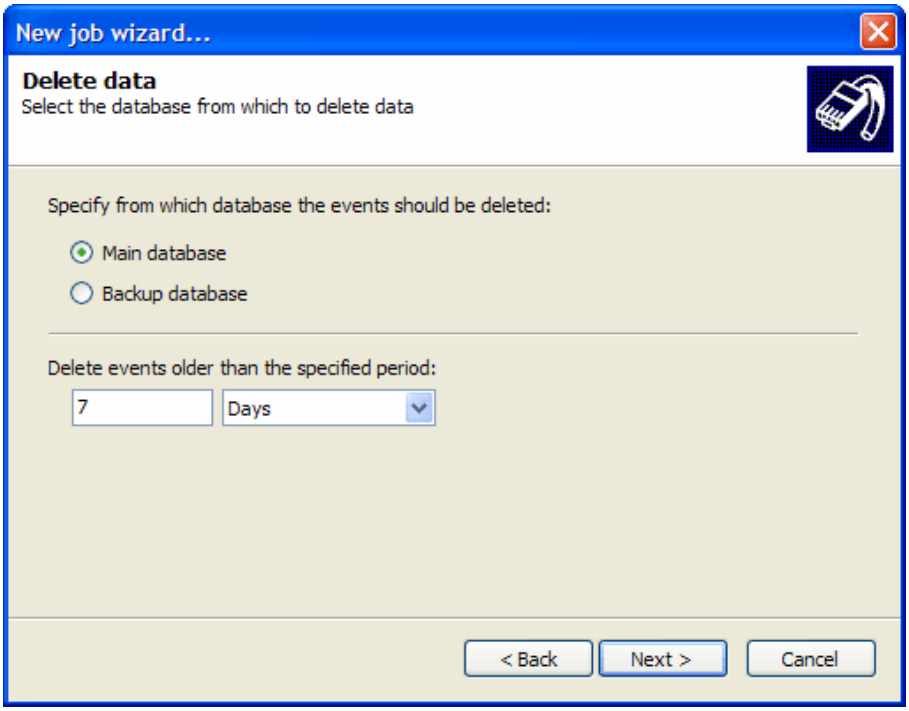
Hinweis: Bei erfolgreich importierten Dateien wird die Dateierweiterung von EXP in IMP geändert.

Aufgabe „Delete data“ (Daten löschen)

So löschen Sie Ereignisse aus der Haupt-Datenbank:

1. Starten Sie den Assistenten für neue Wartungsaufgaben, wie oben unter „Einrichten einer Wartungsaufgabe“ beschrieben, und wählen Sie die Aufgabe **Delete data**.

Hinweis: Wichtige Ereignisse sollten durch die Wartungsaufgaben **Move to database** oder **Export to file** gesichert werden, bevor die Aufgabe **Delete data** durchgeführt wird. Gelöschte Ereigniseinträge können *nicht* wiederhergestellt werden.



Screenshot 105 – Assistent zum Einrichten einer neuen Wartungsaufgabe: Aufgabe „Delete data“ (Daten löschen)

2. Legen Sie fest, ob Ereignisse aus der Haupt- oder Backend-Datenbank gelöscht werden sollen.

3. Legen Sie mit der Option **Delete events older than the specified period** fest, dass nur vor dem angegebenen Zeitraum eingetretene Ereignisse gelöscht werden.

4. Klicken Sie auf die Schaltfläche **Next**, um weitere Filterbedingungen für Ereignisdaten zu definieren.

5. Legen Sie weitere Bedingungen für diese Filteraufgabe fest. Andernfalls werden alle Ereignisse, die älter sind als von Ihnen festgelegt, gelöscht. Klicken Sie auf die Schaltfläche **Next**.

Hinweis: Weitere Informationen zur Festlegung von Filter-bedingungen erhalten Sie unter „Konfigurieren der Datenfilter-Bedingungen" in diesem Kapitel.

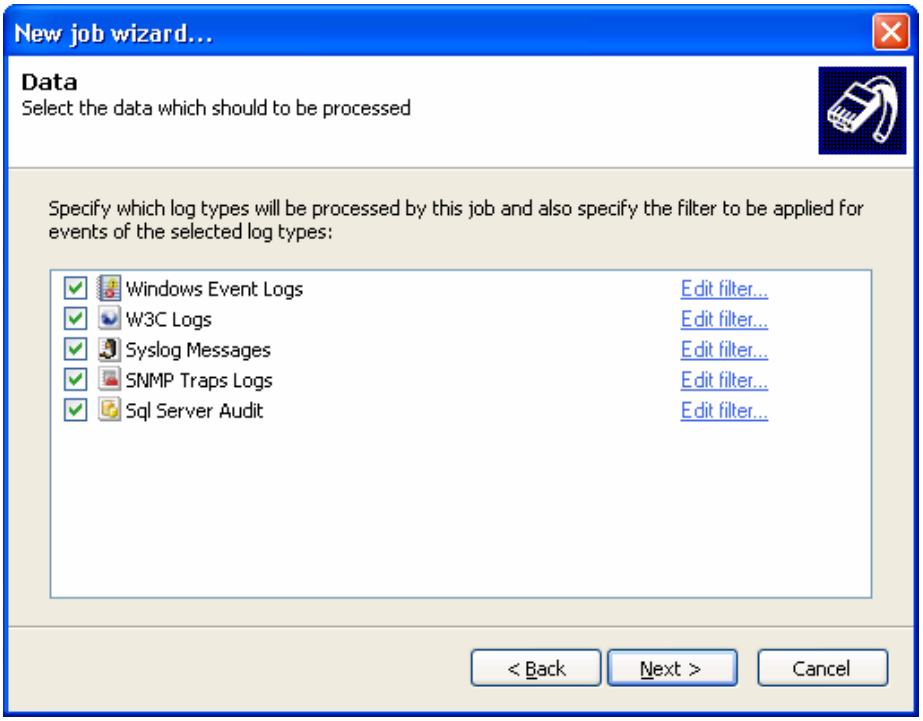
6. Legen Sie fest, ob die Wartungsaufgabe nach Zeitplan oder sofort und nur einmalig durchzuführen ist.

7. Klicken Sie auf die Schaltfläche **Finish**, um die Konfigurierung der Wartungsaufgabe zu beenden.

Konfigurieren der Datenfilter-Bedingungen

Durch das Konfigurieren von Filtern einer Wartungsaufgabe können Ereignisdaten noch gezielter bearbeitet werden. Sie haben die Möglichkeit, nur solche Ereignisse verarbeiten, verschieben, exportieren, löschen oder importieren zu lassen, die mit von Ihnen angegebenen Filterbedingungen übereinstimmen.

- Filter können für alle unterstützten Protokolltypen eingerichtet werden.


New job wizard...
Data
Select the data which should to be processed
Specify which log types will be processed by this job and also specify the filter to be applied for events of the selected log types:
Windows Event Logs
W3C Logs
Syslog Messages
SNMP Traps Logs
Sql Server Audit
Edit filter...
Edit filter...
Edit filter...
Edit filter...
Edit filter...
< Back
Next >
Cancel

Screenshot 106 – Festlegung zu bearbeitender Protokolltypen

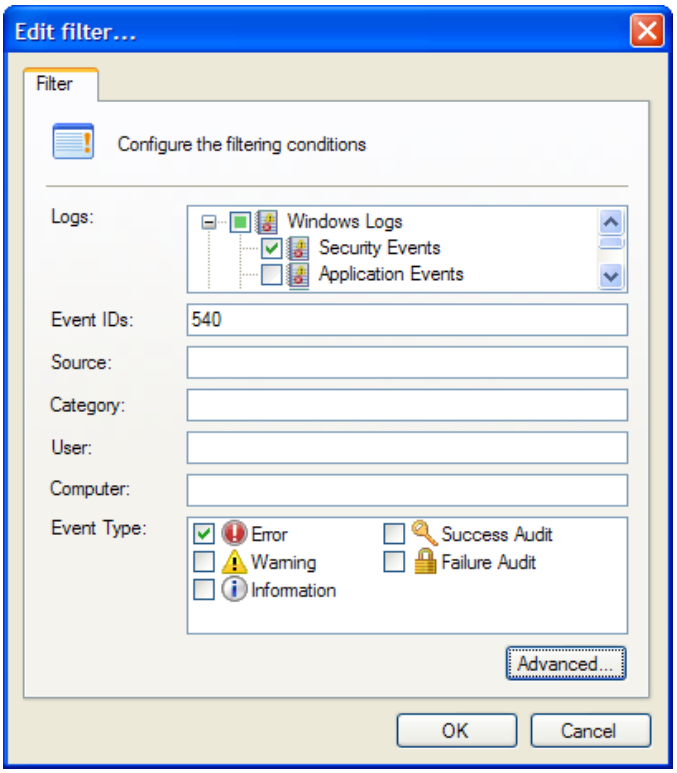
Um genauer zu definieren, welche Ereignisse im Rahmen der Wartungsaufgabe verarbeitet werden sollen, klicken Sie auf den Link **Edit filter** neben dem jeweiligen Protokolltyp.

Beispiel: Filter für Windows-Ereignisprotokolle

Im folgenden Beispiel sollen durch die Festlegung von Bedingungen bestimmte Ereignisse aus dem Sicherheitsprotokoll von Windows exportiert werden:

- **Log type (Protokolltyp):** *Sicherheit*
- **Event ID (Ereignis-ID):** *540 – erfolgreiche Anmeldung*
- **User (Benutzer):** *Administrator*
- **Event Type (Ereignistyp):** *Error (Fehler).*

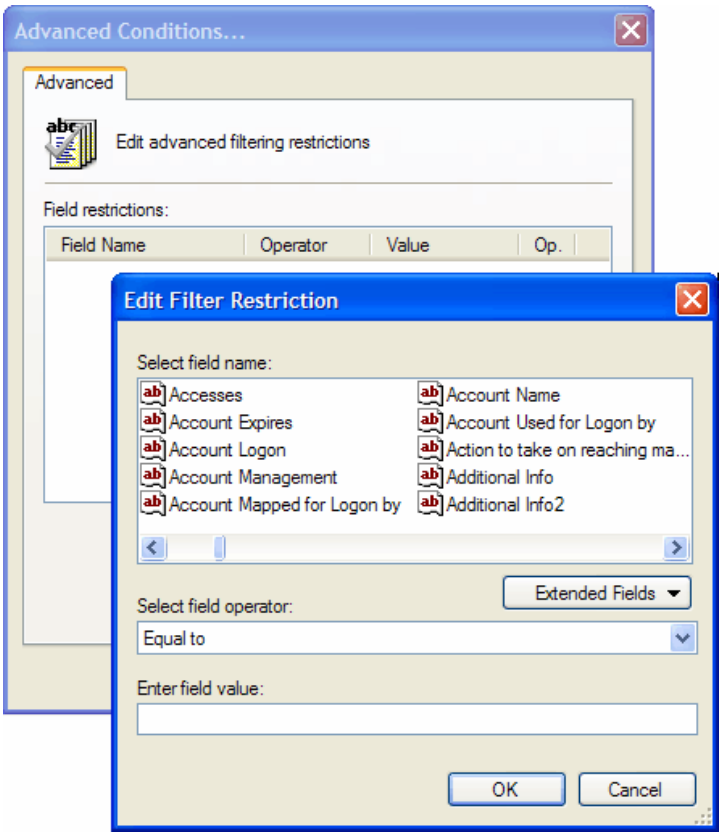
Die hierfür notwendigen Filtereinstellungen sind wie im folgenden Screenshot dargestellt zu konfigurieren:



Screenshot 107 – Erstellen eines Filters für Windows-Ereignisse

Klicken Sie auf die Schaltfläche **OK**, um die Filtereinstellungen zu bestätigen.

Erweiterte Filterbedingungen

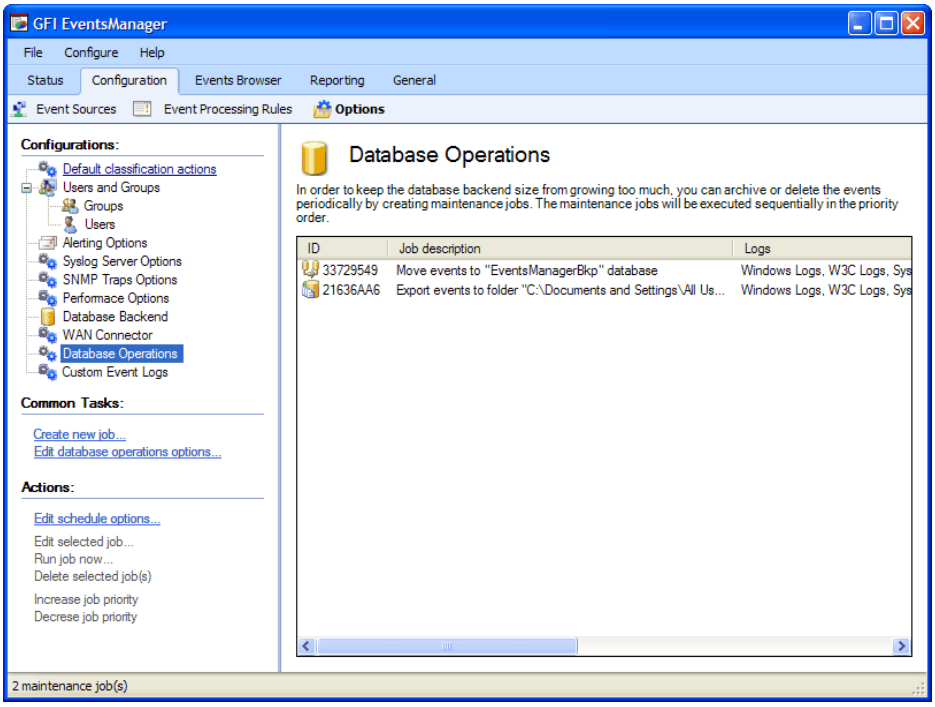


Screenshot 108 – Erweiterte Filterbedingungen

Über den Dialog **Edit filter** lassen sich per Schaltfläche **Advanced** erweiterte Filterbedingungen festlegen. Sie erlauben es Ihnen, Filter auf alle von GFI EventsManager verwendeten Ereignis-Datenfelder anzuwenden.

Hinweis: Filter lassen sich auch für bereits erstellte Wartungsaufgaben einrichten und bearbeiten. Weitere Informationen hierzu erhalten Sie unter „Bearbeiten einer Wartungsaufgabe“.

Anzeigen geplanter Wartungsaufgaben



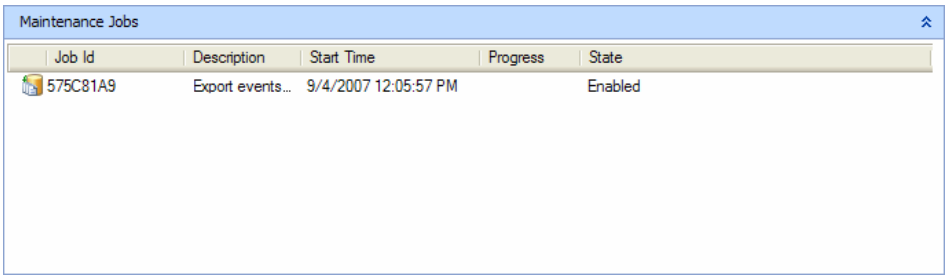
Screenshot 109 – Anzeigen geplanter Wartungsaufgaben

So zeigen Sie geplante Wartungsaufgaben an:

1. Klicken Sie auf den Reiter **Configuration** ▸ **Options**.

2. Klicken Sie im linken Fensterbereich auf den Knoten **Database Operations**. Geplante Wartungsaufgaben werden im rechten Fensterbereich angezeigt.

Statusanzeige zu Wartungsprozessen



Screenshot 110 – Bereich „Maintenance Jobs“

Klicken Sie auf den Reiter **Status** und wählen Sie die Ansicht **Job Activity**, um im Bereich **Maintenance Jobs** den Fortschritt aktuell durchgeführter Wartungsaufgaben zu verfolgen.

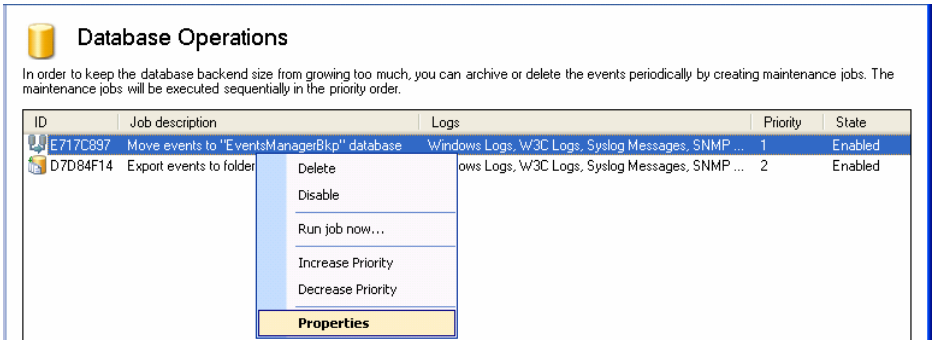
Bearbeiten einer Wartungsaufgabe

So bearbeiten Sie die Einstellungen von geplanten Wartungsaufgaben:

1. Klicken Sie auf den Reiter **Configuration ▸ Options**.

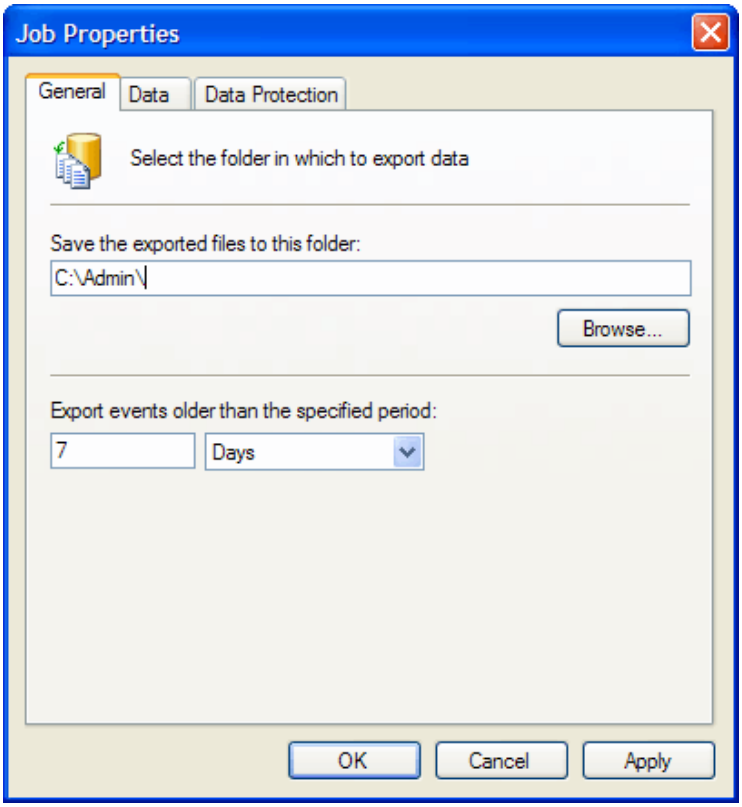
2. Klicken Sie im linken Fensterbereich auf den Knoten **Database Operations**.

3. Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf die zu bearbeitende Wartungsaufgabe. Wählen Sie im Kontextmenü **Properties**.



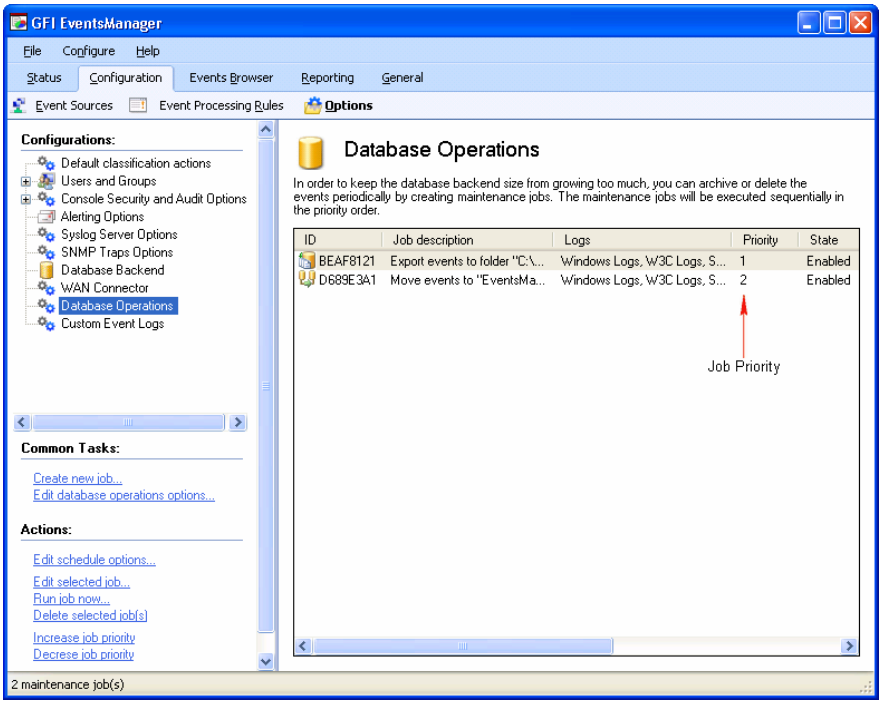
Screenshot 111 – Bearbeiten einer Wartungsaufgabe

4. Führen Sie die gewünschten Änderungen durch und klicken Sie auf die Schaltfläche **OK**, um die Einstellungen zu speichern.



Screenshot 112 – Änderung von Einstellungen eines geplanten Wartungsauftrags

Ändern der Priorität einer Wartungsaufgabe


GFI EventsManager
File Configure Help
Status Configuration Events Browser Reporting General
Event Sources Event Processing Rules Options
Configurations:
Default classification actions
Users and Groups
Console Security and Audit Options
Alerting Options
Syslog Server Options
SNMP Traps Options
Database Backend
WAN Connector
Database Operations
Custom Event Logs
Common Tasks:
Create new job...
Edit database operations options...
Actions:
Edit schedule options...
Edit selected job...
Run job now...
Delete selected job(s)
Increase job priority
Decrese job priority
Database Operations
In order to keep the database backend size from growing too much, you can archive or delete the events periodically by creating maintenance jobs. The maintenance jobs will be executed sequentially in the priority order.
ID Job description Logs Priority State
BEAF8121 Export events to folder "C:\... Windows Logs, W3C Logs, S... 1 Enabled
D689E3A1 Move events to "EventsMa... Windows Logs, W3C Logs, S... 2 Enabled
Job Priority
2 maintenance job(s)

Screenshot 113 – Priorität einer Wartungsaufgabe

Wartungsaufgaben werden standardmäßig in der Reihenfolge ausgeführt, in der sie erstellt wurden. Die zuerst erstellte Aufgabe erhält somit die höchste Priorität.

Falls erforderlich, können Sie die Dringlichkeit der Ausführung einer Aufgabe erhöhen oder senken:

1. Klicken Sie auf den Reiter **Configuration** ▸ **Options**.

2. Klicken Sie im linken Fensterbereich auf den Knoten **Database Operations**.

3. Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf die Wartungsaufgabe. Wählen Sie im Kontextmenü **Increase Priority** zum Erhöhen oder **Decrease Priority** zum Senken der Priorität.

Löschen einer Wartungsaufgabe

So löschen Sie noch nicht durchgeführte Wartungsaufgaben:

1. Klicken Sie auf den Reiter **Configuration** ▸ **Options**.

2. Klicken Sie im linken Fensterbereich auf den Knoten **Database Operations**.

3. Klicken Sie im rechten Fenster mit der rechten Maustaste auf die zu löschende Wartungsaufgabe und wählen Sie im Kontextmenü **Delete**.

Wichtig: Wartungsaufgaben sollten mit Vorsicht gelöscht werden, da dieser Vorgang sich indirekt auf Ereignisdaten auswirkt. Beispiel: Einer Aufgabe **Export to file** ist eine höhere Priorität zugewiesen worden als einer Aufgabe **Delete data**. Wird die Aufgabe **Export to file** gelöscht, kann die nachfolgende Aufgabe dazu führen, dass Ereignisdaten entfernt werden, ohne dass diese zuvor gesichert worden sind.

Anpassen von Regeln zur Ereignisverarbeitung

Einführung

Regeln zur Ereignisverarbeitung sichern die Ausführung folgender Aufgaben:

- Klassifizierung von verarbeiteten Ereignissen
- Herausfilterung von sich wiederholenden oder unerwünschten Ereignissen
- Versand von Warnungen bei wichtigen Ereignissen (per E-Mail, SMS und Netzwerknachricht)
- Durchführung von Gegenmaßnahmen durch das Ausführen von Skripten und ausführbaren Dateien bei wichtigen Ereignissen

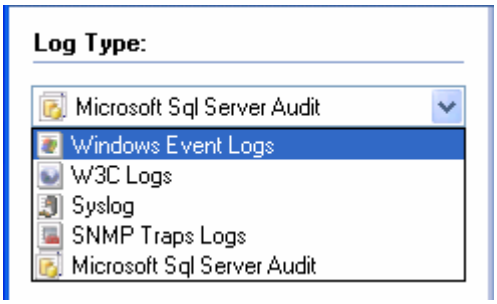
GFI EventsManager bietet bereits vordefinierte Regeln, mit denen sich Ereignisse ohne großen Konfigurationsaufwand verarbeiten lassen. Diese Standardregeln lassen sich an eigene Anforderungen anpassen. Ebenso können Sie neue Regeln für alle unterstützten Protokolltypen erstellen (Windows-Ereignisprotokolle, W3C-Protokolle, Syslog-Meldungen, SNMP-Traps und SQL-Server-Audits).

GFI EventsManager verwaltet Regeln zur Ereignisverarbeitung in Regelsätzen, die wiederum in speziellen Regelsatz-Ordnern organisiert werden. Bereits mitgelieferte Standardregeln werden über die nachfolgenden Regelsatz-Ordner verwaltet:

Regelsatz-Ordner	Beschreibung
Noise Reduction (Noise-Reduzierung)	Regeln entfernen sich wiederholende und irrelevante Ereignisse aus Protokollen
PCI Requirements Windows OS (PCI-Anforderungen – Windows-Betriebssysteme)	Regeln zur Einhaltung der PCI DSS-Compliance (Payment Card Industry Data Security Standard)
Security (Sicherheit)	Regeln verarbeiten Sicherheits- und Systemprotokolle
System Health (Systemzustand)	Regeln verarbeiten Anwendungs- und Systemprotokolle
Security Applications (Sicherheitsanwendungen)	Regeln verarbeiten Anwendungs-, Sicherheits- und Systemprotokolle
Infrastructure Server (Infrastruktur-Server)	Regeln verarbeiten Anwendungs-, DNS-Server- und Systemprotokolle
Database Server (Datenbank-Server)	Regeln verarbeiten Anwendungsprotokolle

Web Server (Webserver)	Regeln verarbeiten Anwendungs- und Systemprotokolle
Print Server (Drucker-Server)	Regeln verarbeiten Anwendungs- und Systemprotokolle
Terminal Services (Terminal-Dienste)	Regeln verarbeiten Ereignisse von Terminal-Gerätetreibern
Email Server	Regeln verarbeiten Ereignisse von Microsoft Exchange-Servern
File Replication (Dateireplikation)	Regeln verarbeiten Ereignisse von Diensten zur Dateireplikation
Directory Service (Verzeichnisdienst)	Regeln verarbeiten Ereignisse aus dem Verzeichnisdienst-Protokoll
HTTP Protocol Logs (HTTP-Ereignisse)	Regeln verarbeiten von IIS-Webservern protokollierte HTTP-Ereignisse
FTP Protocol Logs (FTP-Ereignisse)	Regeln verarbeiten von IIS-Webservern protokollierte FTP-Ereignisse
SMTP Protocol Logs (SMTP-Ereignisse)	Regeln verarbeiten von IIS SMTP-Servern protokollierte Ereignisse
Linux/Unix	Regeln verarbeiten Syslog-Meldungen
Cisco PIX & ASA	Regeln verarbeiten Ereignisse von Cisco PIX-Firewalls und Cisco Adaptive Security Applicances

Erstellen eines neuen Regelsatz-Ordners



Screenshot 114 – Auswahl von Protokolltypen

So erstellen Sie einen neuen Regelsatz-Ordner :

1. Klicken Sie auf den Reiter **Configuration** ▸ **Events Processing Rules**.

2. Wählen Sie aus der angezeigten Drop-Down-Liste den Protokolltyp aus, für den der Regelsatz-Ordner erstellt werden soll.

3. Wählen Sie im linken Fensterbereich unter **Common Tasks** die Option **Create folder** aus.

4. Geben Sie dem neuen Regelsatz-Ordner einen eindeutigen Namen.

Umbenennen und Löschen von Ordnern

Klicken Sie mit der rechten Maustaste auf den Regelsatz-Ordner und wählen Sie im Kontextmenü zum Umbenennen des Ordners **Rename** bzw. zum Löschen **Delete**.

Hinweis: Durch das Löschen eines Regelsatz-Ordners werden alle darin enthaltenen Regeln und Regelsätze gelöscht.

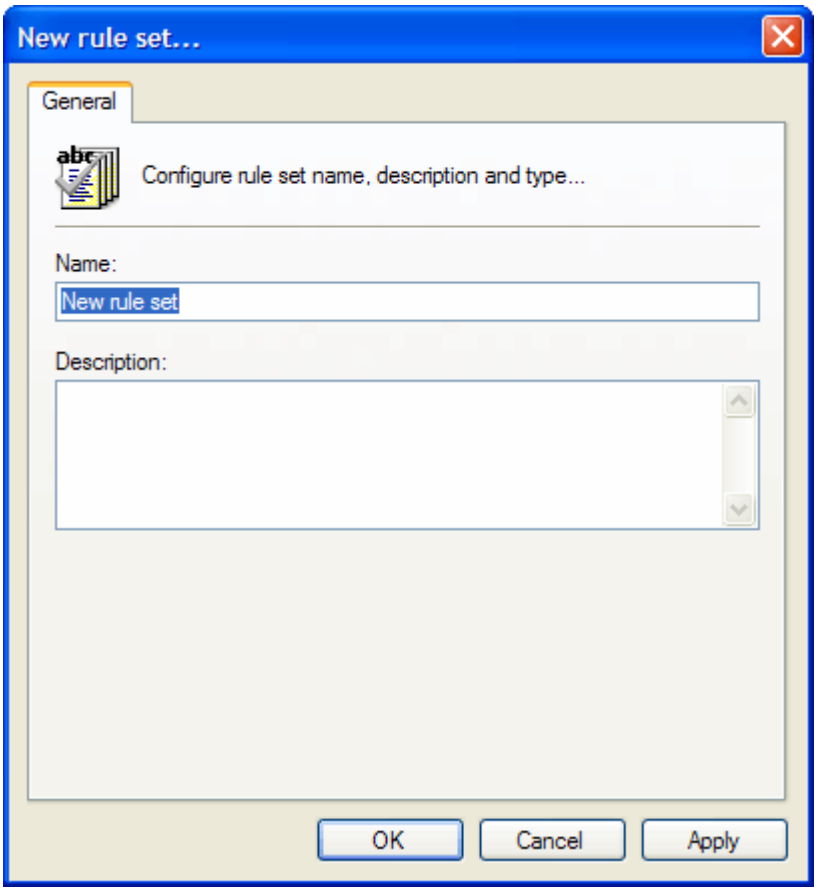
Erstellen eines neuen Regelsatzes

So erstellen Sie einen neuen Regelsatz:

1. Klicken Sie auf den Reiter **Configuration ▸ Events Processing Rules**.

2. Wählen Sie aus der angezeigten Drop-Down-Liste den Protokolltyp aus, für den der Regelsatz erstellt werden soll.

3. Klicken Sie mit der rechten Maustaste auf den Ordner, in dem der neue Regelsatz erstellt werden soll, und wählen Sie im Kontextmenü **Create new rule set** aus.



Screenshot 115 – Erstellen eines neuen Regelsatzes

4. Geben Sie dem Regelsatz einen Namen und eine Beschreibung.

5. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen fertig zu stellen.

Bearbeiten eines Regelsatzes

So bearbeiten Sie die Einstellungen eines Regelsatzes:

1. Klicken Sie mit der rechten Maustaste auf den zu verändernden Regelsatz und wählen Sie im Kontextmenü **Properties**.

2. Führen Sie die gewünschten Änderungen durch und klicken Sie auf die Schaltfläche **OK**, um die Einstellungen fertig zu stellen.

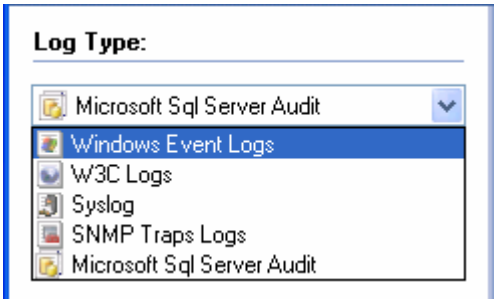
Löschen eines Regelsatzes

Klicken Sie mit der rechten Maustaste auf einen Regelsatz und wählen Sie im Kontextmenü **Delete**, um ihn zu löschen.

Erstellen einer neuen Regel für Windows-Ereignisprotokolle

So erstellen Sie eine neue Regel, die nur für Windows-Ereignis-protokolle gilt:

1. Klicken Sie auf den Reiter **Configuration ▸ Events Processing Rules**.

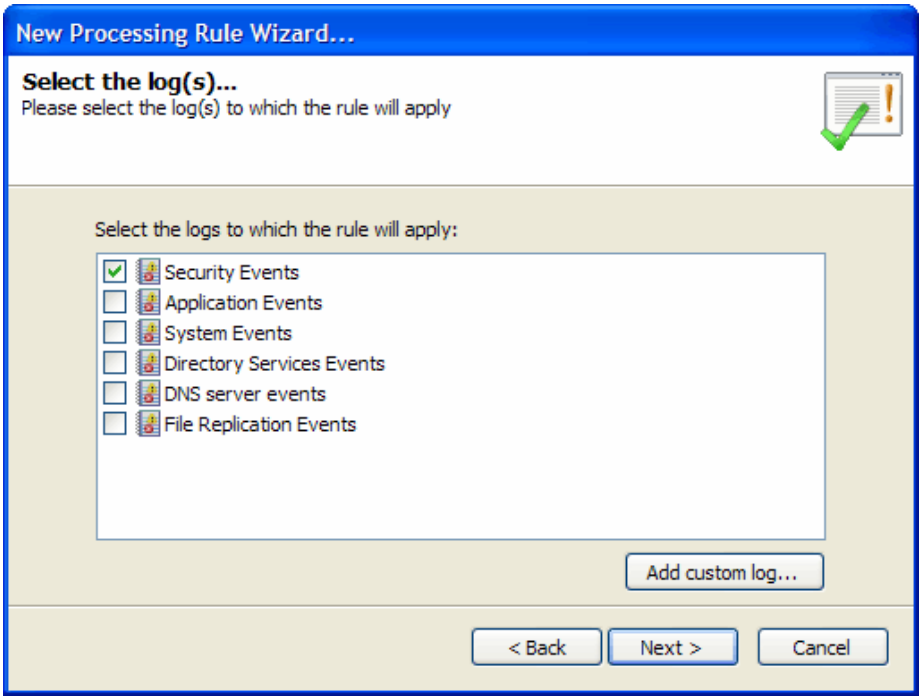


Screenshot 116 – Auswahl des Protokolltyps

2. Wählen Sie aus der angezeigten Drop-Down-Liste den Eintrag **Windows Event Logs** aus.

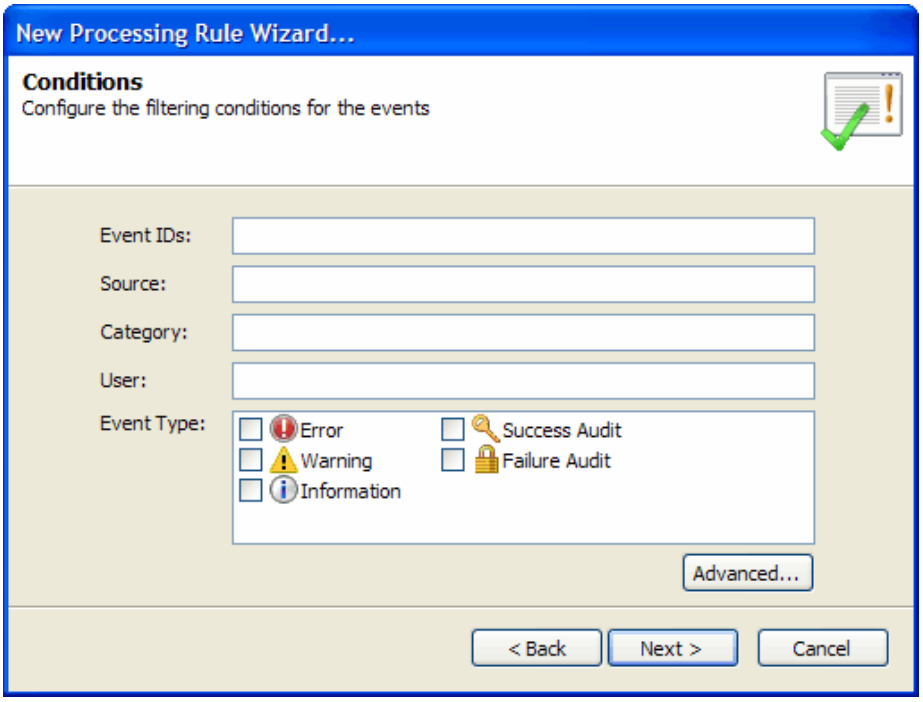
3. Klicken Sie mit der rechten Maustaste auf den Regelsatz, für den die neue Regel erstellt werden soll, und wählen Sie im Kontextmenü **Create new rule…**

4. Geben Sie den Namen und die Beschreibung der neuen Regel an. Klicken Sie auf die Schaltfläche **Next**, um mit der Konfigurierung fortzufahren.



Screenshot 117 – Protokollauswahl

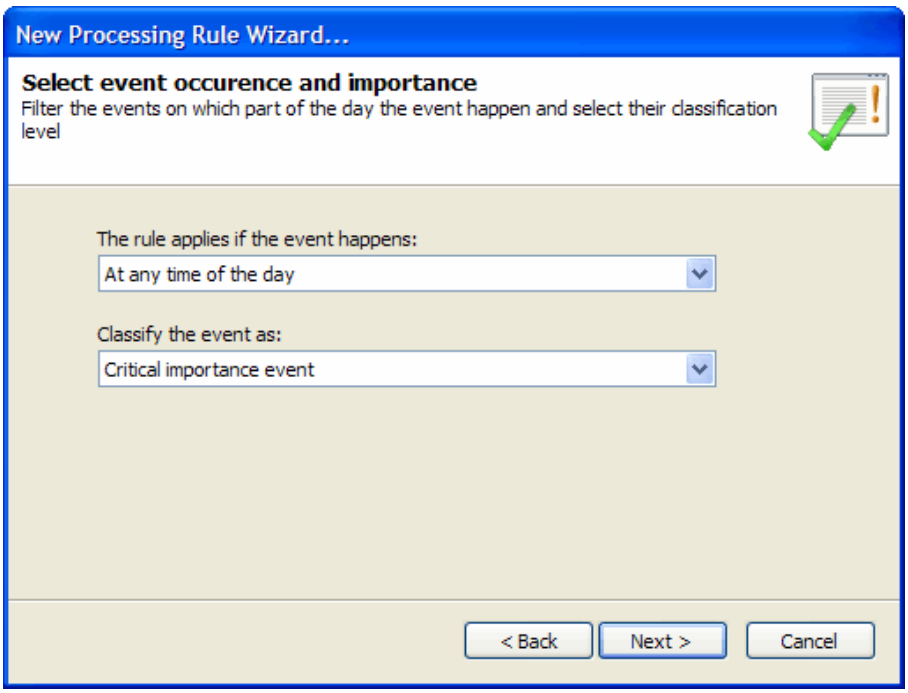
5. Wählen Sie die Ereignisprotokolle aus, für die die Regel gelten soll, und klicken Sie auf die Schaltfläche **Next**.



Screenshot 118 – Festlegung der Filterbedingungen

6. Legen Sie die Filterbedingungen der Regel fest. Soll eine Regel für alle Ereignisse gelten, lassen Sie das Feld **Event IDs** frei. Klicken Sie auf die Schaltfläche **Next**.

Hinweis: Weitere Informationen zur Festlegung erweiterter Filterbedingungen erhalten Sie im Kapitel „Festlegen erweiterter Einstellungen zur Ereignisfilterung“.

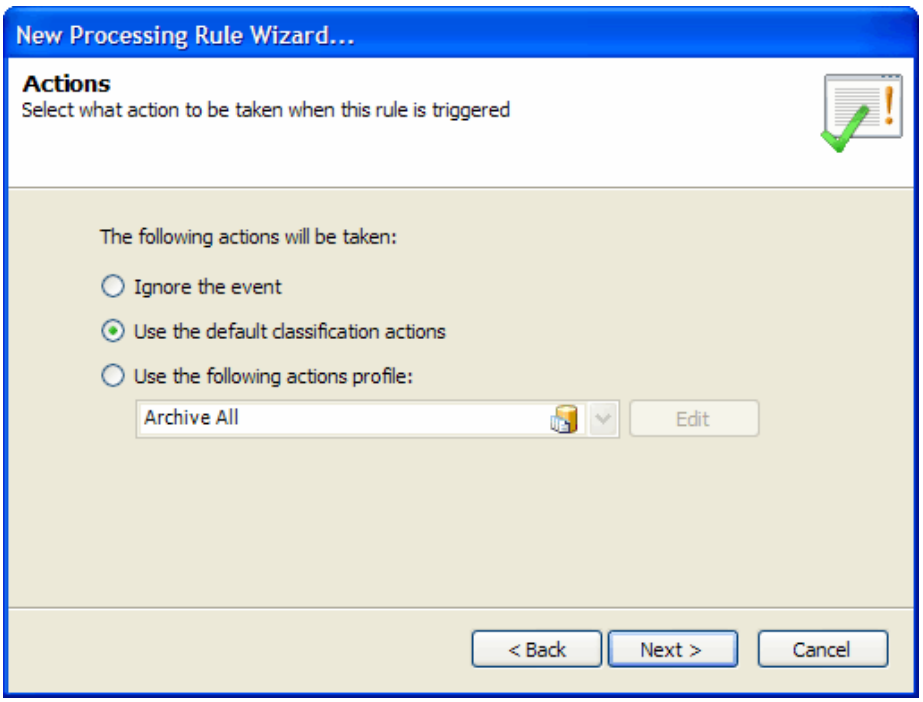

New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
At any time of the day
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Screenshot 119 – Assistent zum Erstellen einer neuen Verarbeitungsregel: Auswahl des Ereigniseintritts und der zuzuweisenden Ereigniskategorie

7. Legen Sie über **The rule applies if the event happens** fest, wann die Regel zur Anwendung kommen soll (jederzeit, während oder außerhalb der regulären Arbeitszeit).

Hinweis: Die Arbeitszeit richtet sich nach der Betriebszeit, die für eine Ereignisquelle definiert wurde. Weitere Informationen zur Festlegung der Betriebszeit finden Sie im Kapitel „Konfigurieren von Ereignisquellen“ unter „Konfigurieren der üblichen Betriebszeit einer Ereignisquelle“.

8. Legen Sie mit **Classify the event as** die Klassifizierung eines Ereignisses fest („critical“ (kritisch), „high“ (hoch), „medium“ (mittel), „low“ (niedrig) oder „Noise“), das die Bedingungen dieser Regel erfüllt. Klicken Sie auf die Schaltfläche **Next**.



Screenshot 120 – Assistent zum Erstellen einer neuen Verarbeitungsregel: Auswahl von Aktionen

9. Legen Sie fest, welche Aktionen von der Regel durchgeführt werden sollen. Durch Auswahl von **Ignore the event** wird das Ereignis ignoriert, per **Use the default classification actions** kann eine klassifizierungsabhängige Standardaktion erfolgen und per **Use the following actions profile** wird ein anpassbares Aktionsprofil verwendet.

10. Klicken Sie auf die Schaltfläche **Next**, um das Fenster zum Abschluss der Konfigurierung aufzurufen. Klicken Sie auf die Schaltfläche **Finish**, um die Einstellungen zu speichern.

Hinweis: Neu erstellte Regeln sind standardmäßig *deaktiviert* und müssen manuell aktiviert werden. Weitere Informationen zur Aktivierung von Regeln zur Ereignisverarbeitung erhalten Sie im Kapitel „Erfassen und Verarbeiten von Windows-Ereignisprotokollen“.

Erstellen einer neuen Regel für W3C-Protokolle

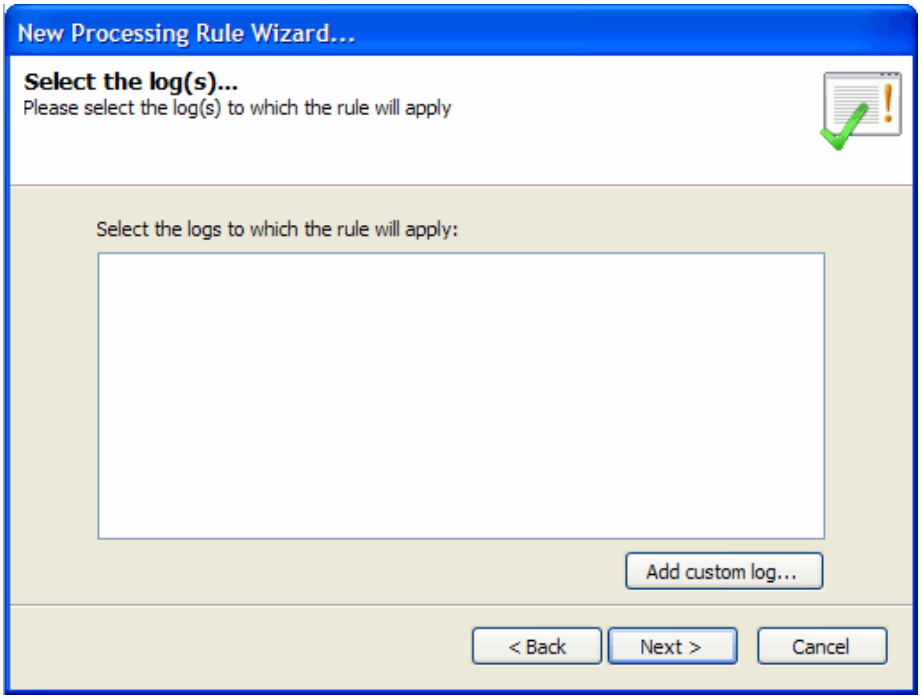
So erstellen Sie eine neue Regel, die nur für W3C-Ereignisprotokolle gilt:

1. Klicken Sie auf den Reiter **Configuration ▸ Events Processing Rules**.

2. Wählen Sie aus der Drop-Down-Liste den Eintrag **W3C Logs** aus.

3. Klicken Sie mit der rechten Maustaste auf den Regelsatz, für den die neue Regel erstellt werden soll, und wählen Sie im Kontextmenü **Create new rule…**

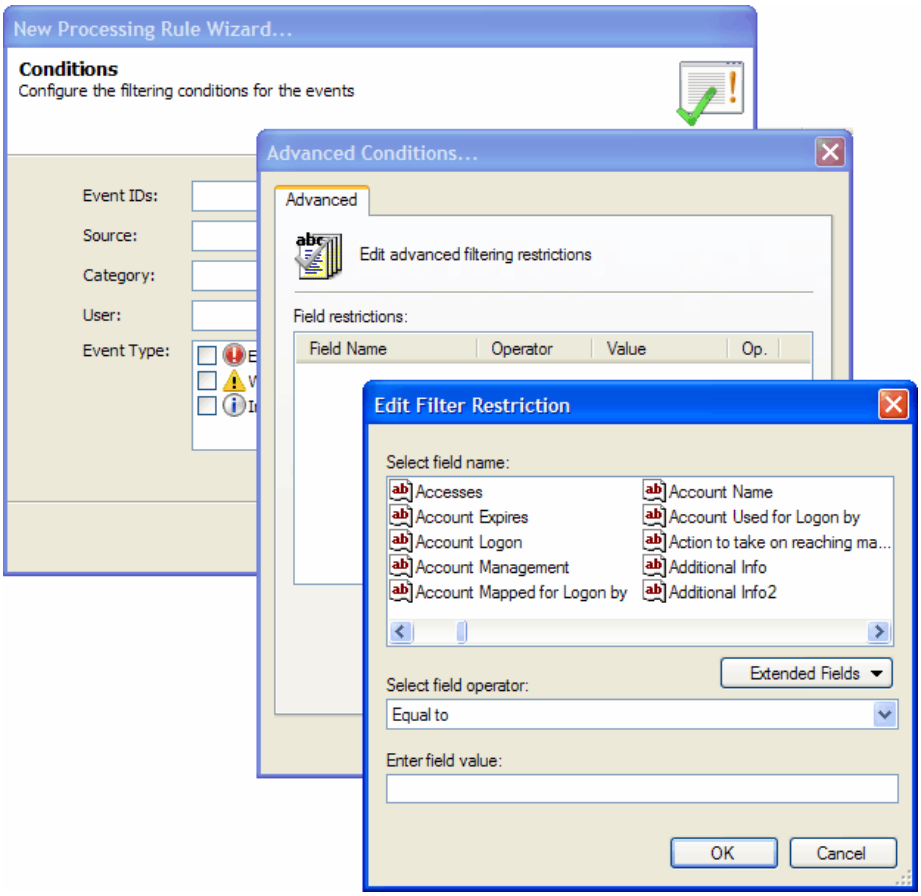
4. Geben Sie den Namen und die Beschreibung der neuen Regel an. Klicken Sie auf die Schaltfläche **Next**.


New Processing Rule Wizard...
Select the log(s)...
Please select the log(s) to which the rule will apply
Select the logs to which the rule will apply:
Add custom log...
< Back
Next >
Cancel

Screenshot 121 – Assistent zum Erstellen einer neuen Verarbeitungsregel: Auswahl des W3C-Protokolls

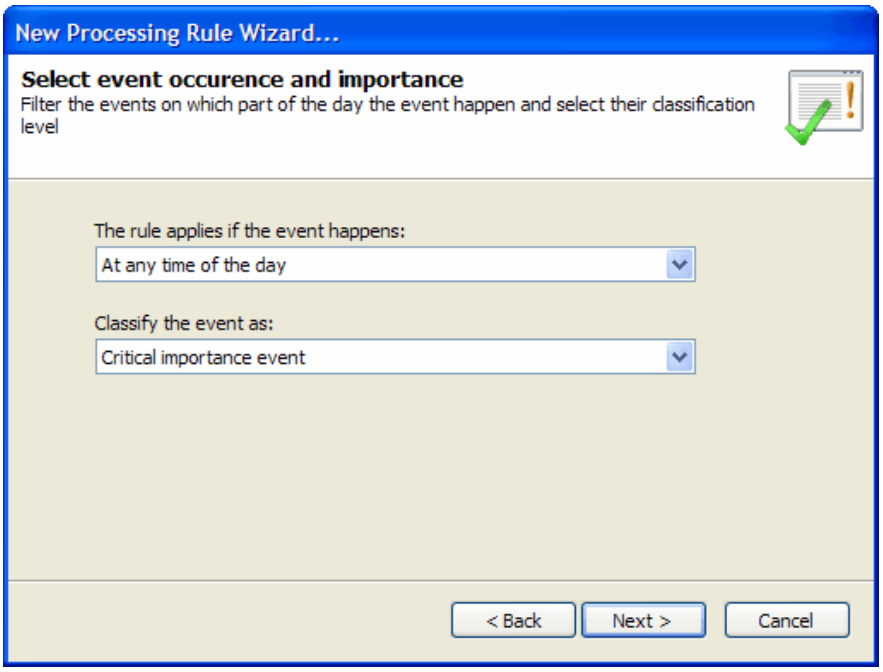
5. Klicken Sie auf die Schaltfläche **Add**. Geben Sie den Dateipfad der W3C-Protokolle an, für das die Regel gelten soll. Wird kein Pfad angegeben, erfolgt die Anwendung der Regel auf alle W3C-Protokolle. Klicken Sie auf die Schaltfläche **Next**.

Hinweis: Es lassen sich mehrere Dateipfade angeben.



Screenshot 122 – Assistent zum Erstellen einer neuen Verarbeitungsregel: Festlegung von Filterbedingungen

6. Klicken Sie auf die Schaltfläche **Add**, um eine Bedingung für die Ereignisfilterung hinzuzufügen. Wiederholen Sie diesen Schritt, bis alle gewünschten Bedingungen festgelegt sind. Klicken Sie auf die Schaltfläche **Next**.

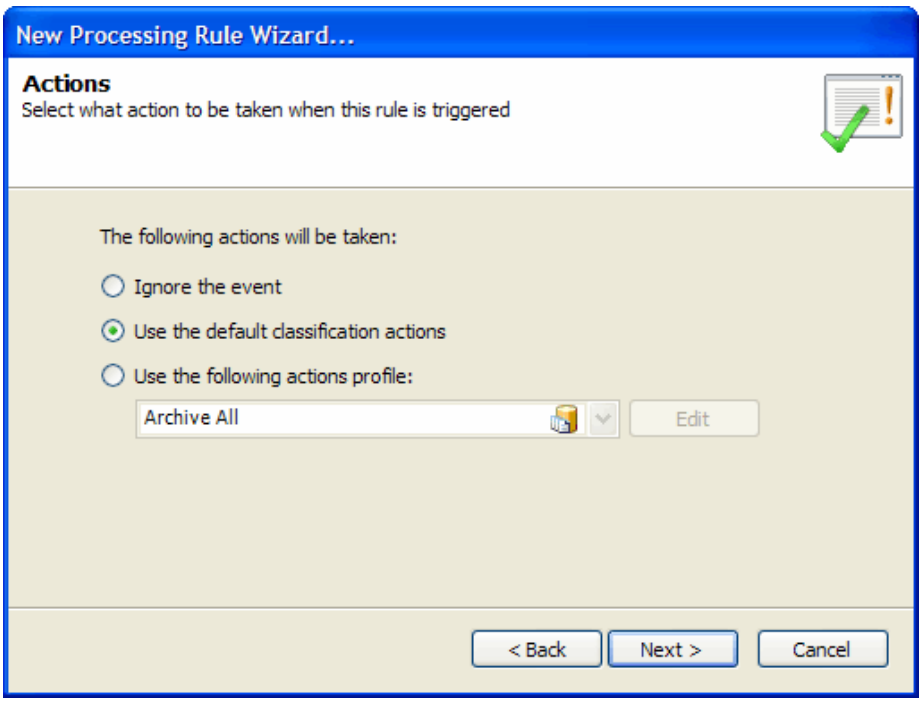

New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
At any time of the day
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Screenshot 123 – Assistent zum Erstellen einer neuen Verarbeitungsregel: Auswahl des Ereigniseintritts und der zuzuweisenden Ereigniskategorie

7. Legen Sie über **The rule applies if the event happens** fest, wann die Regel zur Anwendung kommen soll (jederzeit, während oder außerhalb der regulären Arbeitszeit).

Hinweis: Die Arbeitszeit richtet sich nach der Betriebszeit, die für eine Ereignisquelle definiert wurde. Weitere Informationen zur Festlegung der Betriebszeit finden Sie im Kapitel „Konfigurieren von Ereignisquellen“ unter „Konfigurieren der üblichen Betriebszeit einer Ereignisquelle".

8. Legen Sie mit **Classify the event as** die Klassifizierung eines Ereignisses fest („critical“ (kritisch), „high“ (hoch), „medium“ (mittel), „low“ (niedrig) oder „Noise“), das die Bedingungen dieser Regel erfüllt. Klicken Sie auf die Schaltfläche **Next**.



Screenshot 124 – Assistent zum Erstellen einer neuen Verarbeitungsregel: Auswahl von Aktionen

9. Legen Sie fest, welche Aktionen von der Regel durchgeführt werden sollen. Durch Auswahl von **Ignore the event** wird das Ereignis ignoriert, per **Use the default classification actions** kann eine klassifizierungsabhängige Standardaktion erfolgen und per **Use the following actions profile** wird ein anpassbares Aktionsprofil verwendet.

10. Klicken Sie auf die Schaltfläche **Next**, um das Fenster zum Abschluss der Konfigurierung aufzurufen. Klicken Sie auf die Schaltfläche **Finish**, um die Einstellungen zu speichern.

Hinweis: Neu erstellte Regeln sind standardmäßig *deaktiviert* und müssen manuell aktiviert werden. Weitere Informationen zur Aktivierung von Regeln zur Ereignisverarbeitung erhalten Sie im Kapitel „Erfassen und Verarbeiten von W3C-Protokollen“.

Erstellen einer neuen Syslog-Regel

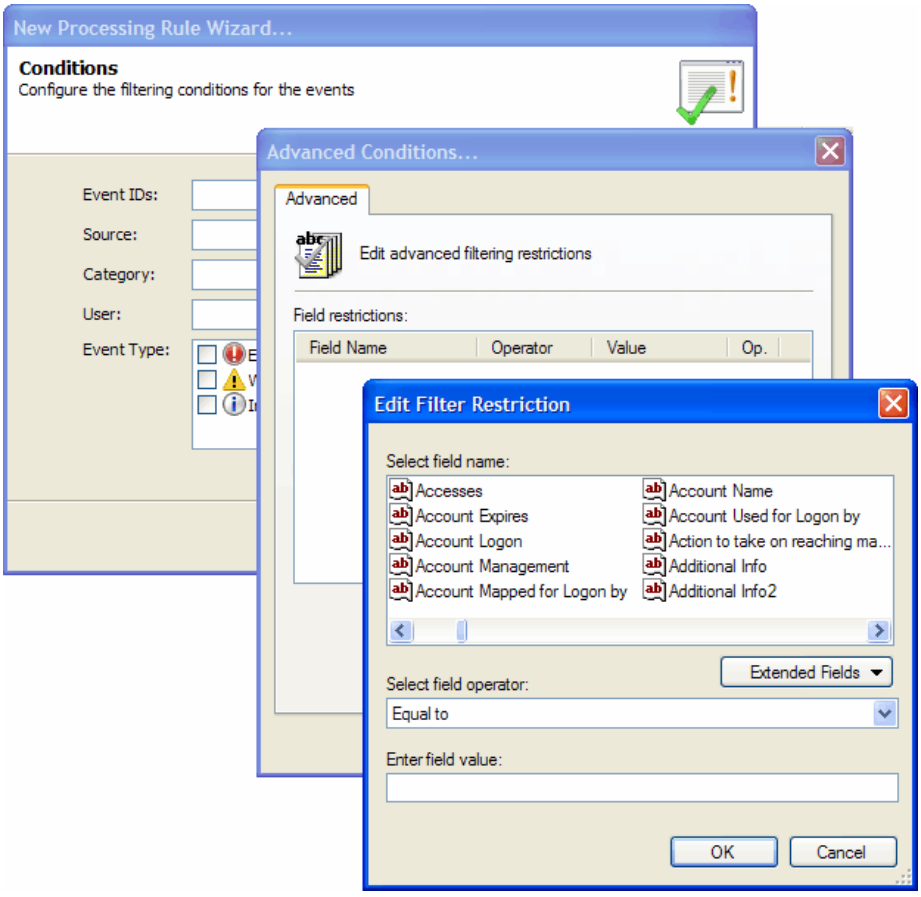
So erstellen Sie eine neue Regel, die nur für die Verarbeitung von Syslog-Meldungen gilt:

1. Klicken Sie auf den Reiter **Configuration ▸ Events Processing Rules**.

2. Wählen Sie aus der Drop-Down-Liste den Eintrag **Syslog** aus.

3. Klicken Sie mit der rechten Maustaste auf den Regelsatz, für den die neue Regel erstellt werden soll, und wählen Sie im Kontextmenü **Create new rule…**

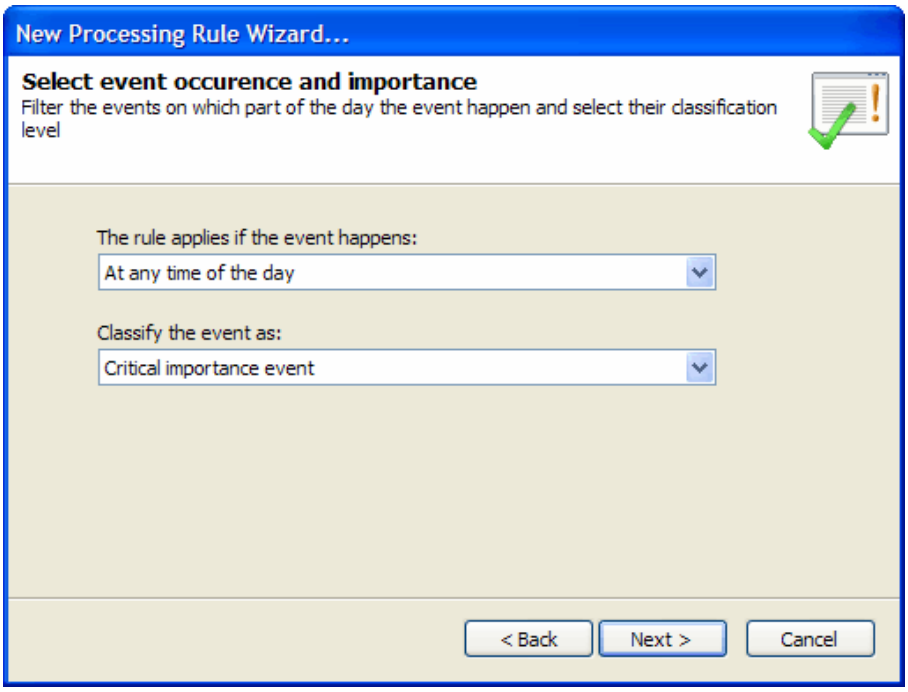
4. Geben Sie den Namen und die Beschreibung der neuen Regel an. Klicken Sie auf die Schaltfläche **Next**.



Screenshot 125 – Assistent zum Erstellen einer neuen Verarbeitungsregel: Festlegung von Filterbedingungen

5. Geben Sie alle im Rahmen dieser Regel zu beachtenden Filterbedingungen an. Klicken Sie auf die Schaltfläche **Next**, nachdem Sie alle Bedingungen festgelegt haben.

Hinweis: Weitere Informationen zur Festlegung erweiterter Filterbedingungen erhalten Sie im Kapitel „Festlegen erweiterter Einstellungen zur Ereignisfilterung".

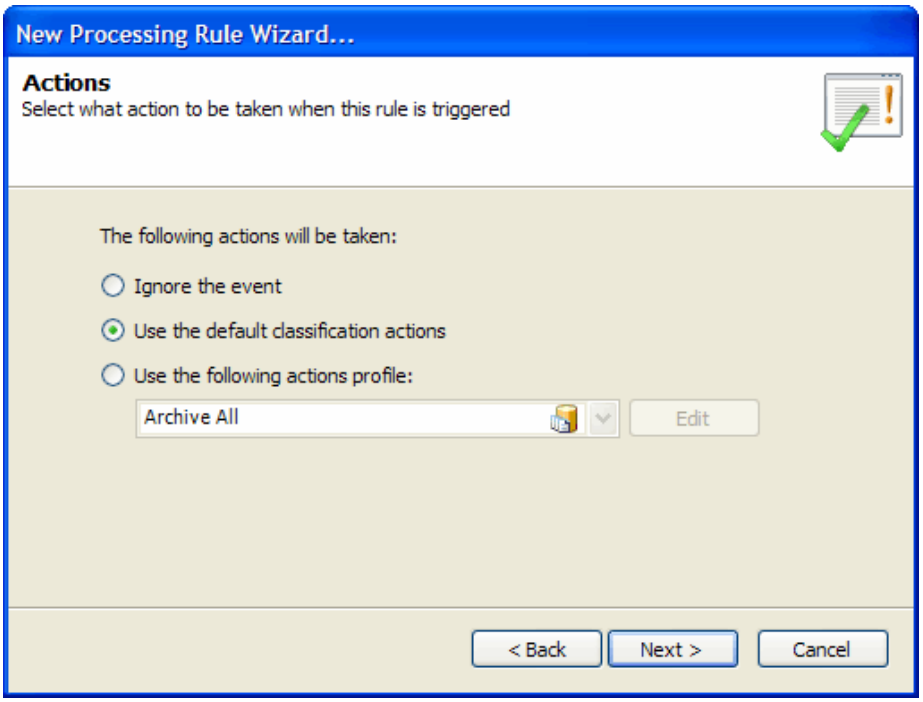

New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
At any time of the day
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Screenshot 126 – Assistent zum Erstellen einer neuen Verarbeitungsregel: Auswahl des Ereigniseintritts und der zuzuweisenden Ereigniskategorie

6. Legen Sie über **The rule applies if the event happens** fest, wann die Regel zur Anwendung kommen soll (jederzeit, während oder außerhalb der regulären Arbeitszeit).

Hinweis: Die Arbeitszeit richtet sich nach der Betriebszeit, die für eine Ereignisquelle definiert wurde. Weitere Informationen zur Festlegung der Betriebszeit finden Sie im Kapitel „Konfigurieren von Ereignisquellen“ unter „Konfigurieren der üblichen Betriebszeit einer Ereignisquelle".

7. Legen Sie mit **Classify the event as** die Klassifizierung eines Ereignisses fest („critical“ (kritisch), „high" (hoch), „medium“ (mittel), „low" (niedrig)), das die Bedingungen dieser Regel erfüllt. Klicken Sie auf die Schaltfläche **Next**.



Screenshot 127 – Assistent zum Erstellen einer neuen Verarbeitungsregel: Auswahl von Aktionen

8. Legen Sie fest, welche Aktionen von der Regel durchgeführt werden sollen. Durch Auswahl von **Ignore the event** wird das Ereignis ignoriert, per **Use the default classification actions** kann eine klassifizierungsabhängige Standardaktion erfolgen und per **Use the following actions profile** wird ein anpassbares Aktionsprofil verwendet.

9. Klicken Sie auf die Schaltfläche **Next**, um die Konfigurierung abzuschließen. Klicken Sie auf die Schaltfläche **Finish**, um die Einstellungen zu speichern.

Hinweis: Neu erstellte Regeln sind standardmäßig *deaktiviert* und müssen manuell aktiviert werden. Weitere Informationen zur Aktivierung von Regeln zur Ereignisverarbeitung erhalten Sie im Kapitel „Erfassen und Verarbeiten von Syslog-Meldungen“.

Erstellen einer neuen Regel für SNMP-Traps

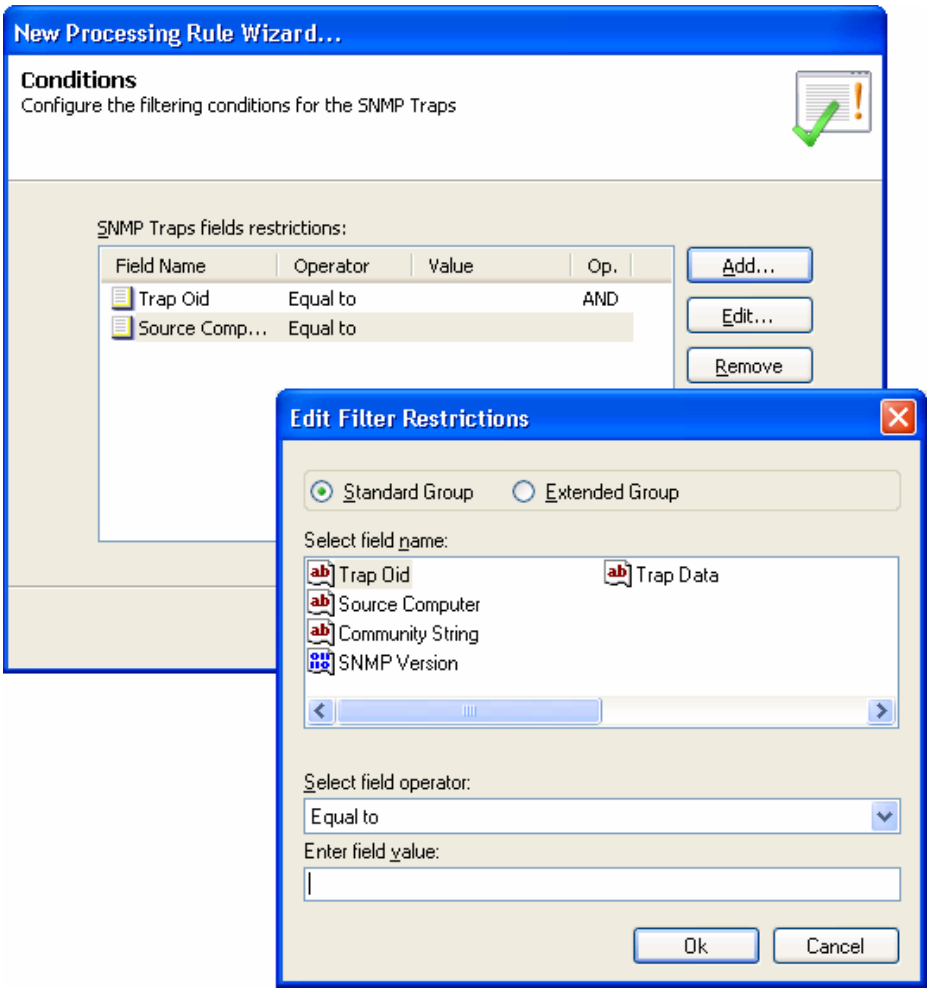
So erstellen Sie eine neue Regel, die nur für die Verarbeitung von SNMP-Traps gilt:

1. Klicken Sie auf den Reiter **Configuration ▸ Events Processing Rules**.

2. Wählen Sie aus der angezeigten Drop-Down-Liste den Eintrag **SNMP Traps Logs** aus.

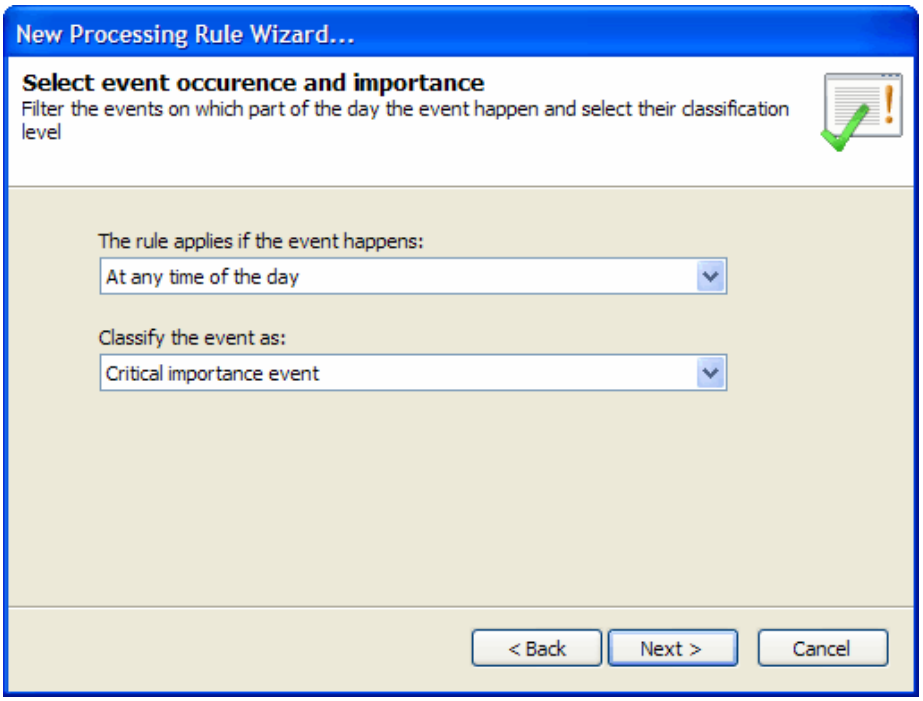
3. Klicken Sie mit der rechten Maustaste auf den Regelsatz, für den die neue Regel erstellt werden soll, und wählen Sie im Kontextmenü **Create new rule…**

4. Geben Sie den Namen und die Beschreibung der neuen Regel an. Klicken Sie auf die Schaltfläche **Next**.



Screenshot 128 – Assistent zum Erstellen einer neuen Verarbeitungsregel: Festlegung von Filterbedingungen

5. Geben Sie alle im Rahmen dieser Regel zu beachtenden Filterbedingungen an. Klicken Sie auf die Schaltfläche **Next**, nachdem Sie alle Bedingungen festgelegt haben.

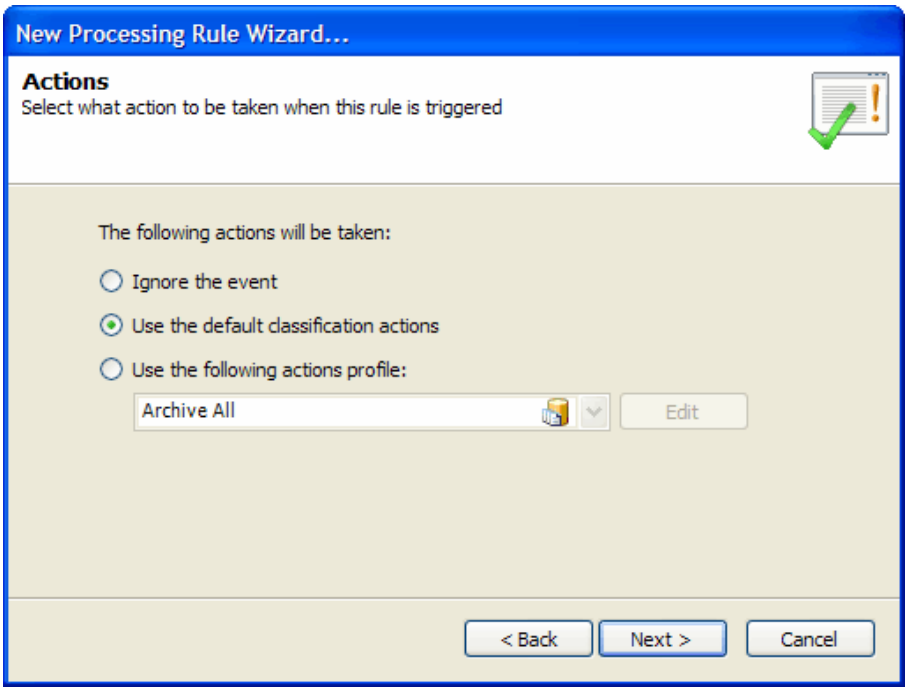

New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
At any time of the day
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Screenshot 129 – Assistent zum Erstellen einer neuen Verarbeitungsregel: Auswahl des Ereigniseintritts und der zuzuweisenden Ereigniskategorie

6. Legen Sie über **The rule applies if the event happens** fest, wann die Regel zur Anwendung kommen soll (jederzeit, während oder außerhalb der regulären Arbeitszeit).

Hinweis: Die Arbeitszeit richtet sich nach der Betriebszeit, die für eine Ereignisquelle definiert wurde. Weitere Informationen zur Festlegung der Betriebszeit finden Sie im Kapitel „Konfigurieren von Ereignisquellen“ unter „Konfigurieren der üblichen Betriebszeit einer Ereignisquelle".

7. Legen Sie mit **Classify the event as** die Klassifizierung eines Ereignisses fest („critical“ (kritisch), „high" (hoch), „medium“ (mittel), „low" (niedrig)), das die Bedingungen dieser Regel erfüllt. Klicken Sie auf die Schaltfläche **Next**.



Screenshot 130 – Assistent zum Erstellen einer neuen Verarbeitungsregel: Auswahl von Aktionen

8. Legen Sie fest, welche Aktionen von der Regel durchgeführt werden sollen. Durch Auswahl von **Ignore the event** wird das Ereignis ignoriert, per **Use the default classification actions** kann eine klassifizierungsabhängige Standardaktion erfolgen und per **Use the following actions profile** wird ein anpassbares Aktionsprofil verwendet.

9. Klicken Sie auf die Schaltfläche **Next**, um das Fenster zum Abschluss der Konfigurierung aufzurufen. Klicken Sie auf die Schaltfläche **Finish**, um die Einstellungen zu speichern.

Hinweis: Neu erstellte Regeln sind standardmäßig *deaktiviert* und müssen manuell aktiviert werden. Weitere Informationen zur Aktivierung von Regeln zur Ereignisverarbeitung erhalten Sie im Kapitel „Erfassen und Verarbeiten von SNMP-Traps“.

Erstellen einer neuen Regel für SQL-Server-Audit-Protokolle

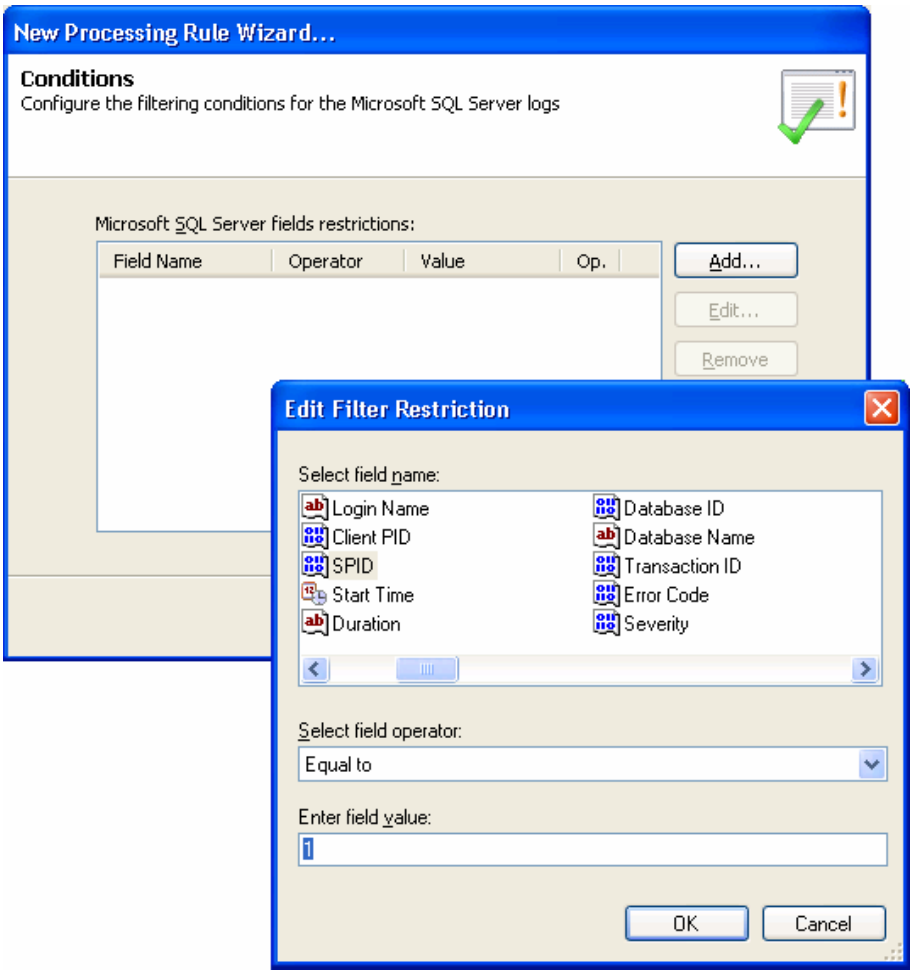
So erstellen Sie eine neue Regel, die nur für die Verarbeitung von Protokollen zu SQL-Server-Audits gilt:

1. Klicken Sie auf den Reiter **Configuration ▸ Events Processing Rules**.

2. Wählen Sie aus der angezeigten Drop-Down-Liste den Eintrag **Microsoft SQL Server Audit** aus.

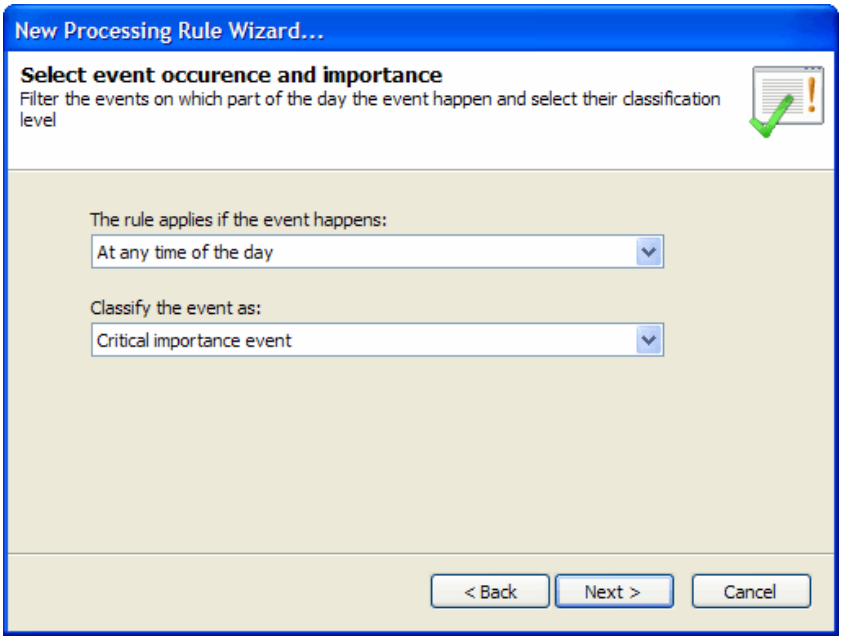
3. Klicken Sie mit der rechten Maustaste auf den Regelsatz, für den die neue Regel erstellt werden soll, und wählen Sie im Kontextmenü **Create new rule…**

4. Geben Sie den Namen und die Beschreibung der neuen Regel an. Klicken Sie auf die Schaltfläche **Next**.



Screenshot 131 – Assistent zum Erstellen einer neuen Verarbeitungsregel: Festlegung von Filterbedingungen

5. Geben Sie alle im Rahmen dieser Regel zu beachtenden Filterbedingungen an. Klicken Sie auf die Schaltfläche **Next**, nachdem Sie alle Bedingungen festgelegt haben.

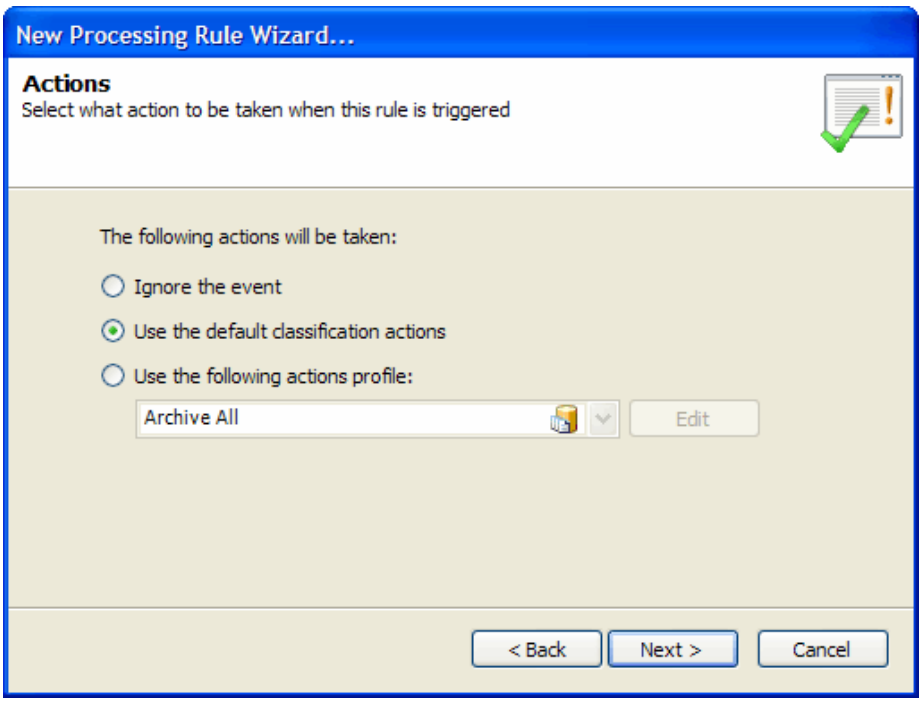

New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
At any time of the day
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Screenshot 132 – Assistent zum Erstellen einer neuen Verarbeitungsregel: Auswahl des Ereigniseintritts und der zuzuweisenden Ereigniskategorie

6. Legen Sie über **The rule applies if the event happens** fest, wann die Regel zur Anwendung kommen soll (jederzeit, während oder außerhalb der regulären Arbeitszeit).

Hinweis: Die Arbeitszeit richtet sich nach der Betriebszeit, die für eine Ereignisquelle definiert wurde. Weitere Informationen zur Festlegung der Betriebszeit finden Sie im Kapitel „Konfigurieren von Ereignisquellen“ unter „Konfigurieren der üblichen Betriebszeit einer Ereignisquelle".

7. Legen Sie mit **Classify the event as** die Klassifizierung eines Ereignisses fest („critical“ (kritisch), „high" (hoch), „medium“ (mittel), „low" (niedrig)), das die Bedingungen dieser Regel erfüllt. Klicken Sie auf die Schaltfläche **Next**.

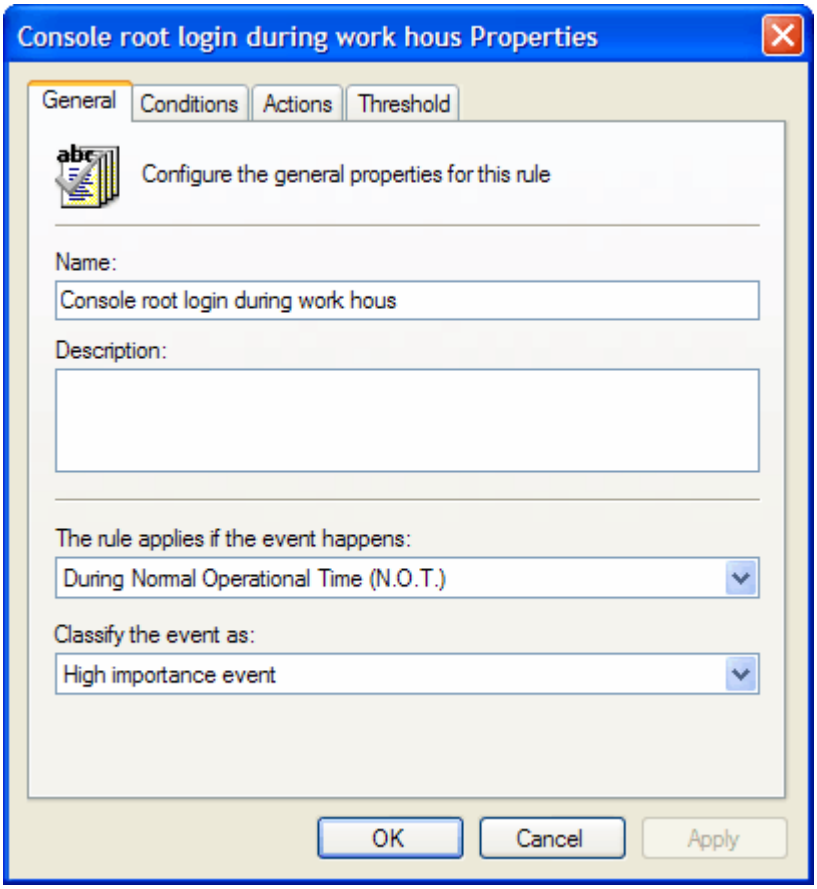


Screenshot 133 – Assistent zum Erstellen einer neuen Verarbeitungsregel: Auswahl von Aktionen

8. Legen Sie fest, welche Aktionen von der Regel durchgeführt werden sollen. Durch Auswahl von **Ignore the event** wird das Ereignis ignoriert, per **Use the default classification actions** kann eine klassifizierungsabhängige Standardaktion erfolgen und per **Use the following actions profile** wird ein anpassbares Aktionsprofil verwendet.

9. Klicken Sie auf die Schaltfläche **Next**, um das Fenster zum Abschluss der Konfigurierung aufzurufen. Klicken Sie auf die Schaltfläche **Finish**, um die Einstellungen zu speichern.

Ändern der Eigenschaften einer Regel



Screenshot 134 – Eigenschaften einer Regel zur Ereignisverarbeitung

So ändern Sie die Eigenschaften einer Regel zur Ereignisverarbeitung:

1. Klicken Sie mit der rechten Maustaste auf die zu bearbeitende Regel und wählen Sie im Kontextmenü **Properties**. Der Dialog zur Anpassung der Regeleigenschaften wird aufgerufen.

2. Über folgende Reiter lassen sich die Regeleigenschaften ändern:

- **General** – Erlaubt die Festlegung allgemeiner Regeleigenschaften wie Name und Klassifizierung.
- **Logs** – Nur für Regeln zu W3C-Protokollen aufrufbar. Geben Sie die W3C-Protokolle an, auf die diese Regel angewendet werden soll.
- **Event Logs** – Nur für Regeln zu Windows-Ereignisprotokollen aufrufbar. Geben Sie an, welche Ereignisse mit dieser Regel verarbeitet werden sollen.
- **Conditions** – Legen Sie Bedingungen zur Ereignisfilterung fest.
- **Actions** – Geben Sie an, welche Warnungen und Aktionen aufgrund dieser Regel erfolgen sollen.
- **Threshold** – Geben Sie an, wie oft ein Ereignis erkannt worden sein muss, bevor Warnungen und Aktionen erfolgen. Hierdurch lassen sich durch Noise ausgelöste Fehlalarme vermeiden.

Festlegen erweiterter Einstellungen zur Ereignisfilterung

Zur differenzierteren Ereignisfilterung stehen weitere Detaileinstellungen zur Verfügung. Diese sind jedoch nur für Windows-Ereignisse und Syslog-Meldungen nutzbar.

Bedingungen für Windows-Ereignisse

Feld „Event IDs“:

Folgende Parameter können über das Feld **Event IDs** angegeben werden:

Parametertyp	Beispiel
Einzelereignis	Event IDs: 575
Lose Folge von Ereignissen	Event IDs: 550, 570
Ereignisbereich	Event IDs: 575-600
Variable Ereignisangabe	Event IDs: 550, 570, 575-600

Felder „Source“, „Category“ und „User“

Folgende Parameter können über die Felder **Source**, **Category** und **User** angegeben werden:

Parametertyp	Beispiel
Name einer Einzelquelle	Source: Userenv
Mehrere Quellen	Source: Userenv, SceCli
Platzhalter (% und *)	Source: S%t%

Syslogspezifische Kategorien

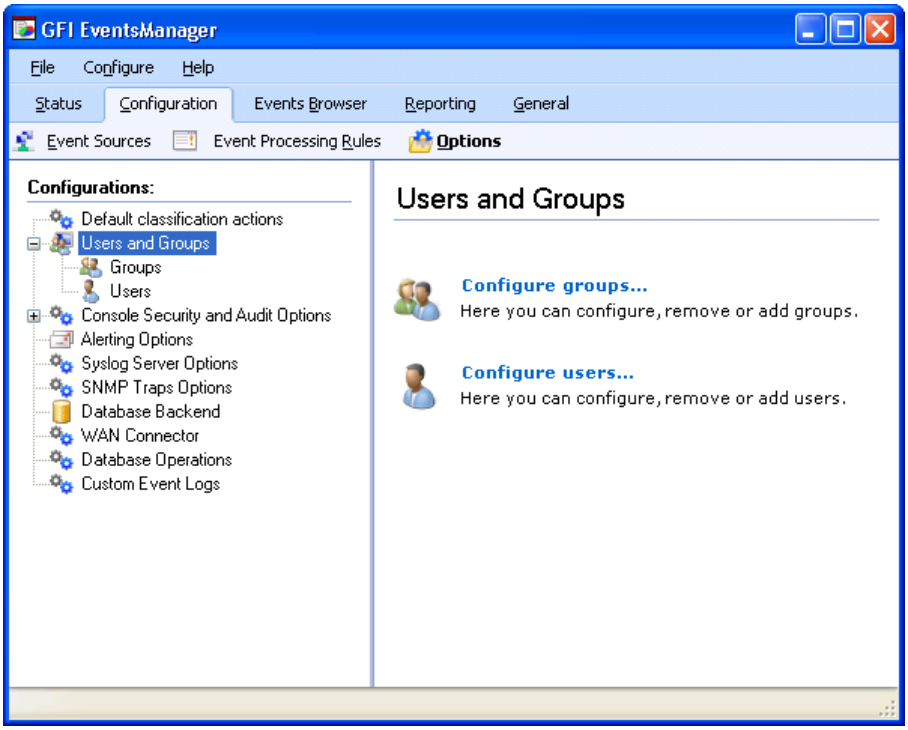
Felder „Message“ und „Process“

Folgende Parameter können über die Felder **Message** und **Process** angegeben werden:

Parametertyp	Beispiel
Einzelne Nachricht	Message: session opened
Mehrere Nachrichten	Message: session opened, session closed
Platzhalter (% und *)	Message: %session opened%

Konfigurieren von Benutzern und Gruppen

Einführung



Screenshot 135 – Konfigurierung von Benutzern und Gruppen

Über den Knoten **Users and Groups** lassen sich GFI EventsManager-Anwendern unterschiedliche Zugriffsrechte für die Verwaltungskonsole zuweisen, ob zur Änderung von Konfigurationseinstellungen oder um lediglich eine Ereignisanzeige zu ermöglichen. Hinzufügen, Ändern oder Löschen von Benutzern und Gruppen sowie wie die Festlegung von Geschäftszeiten und Warnungen erfolgen ebenfalls über diesen Knoten.

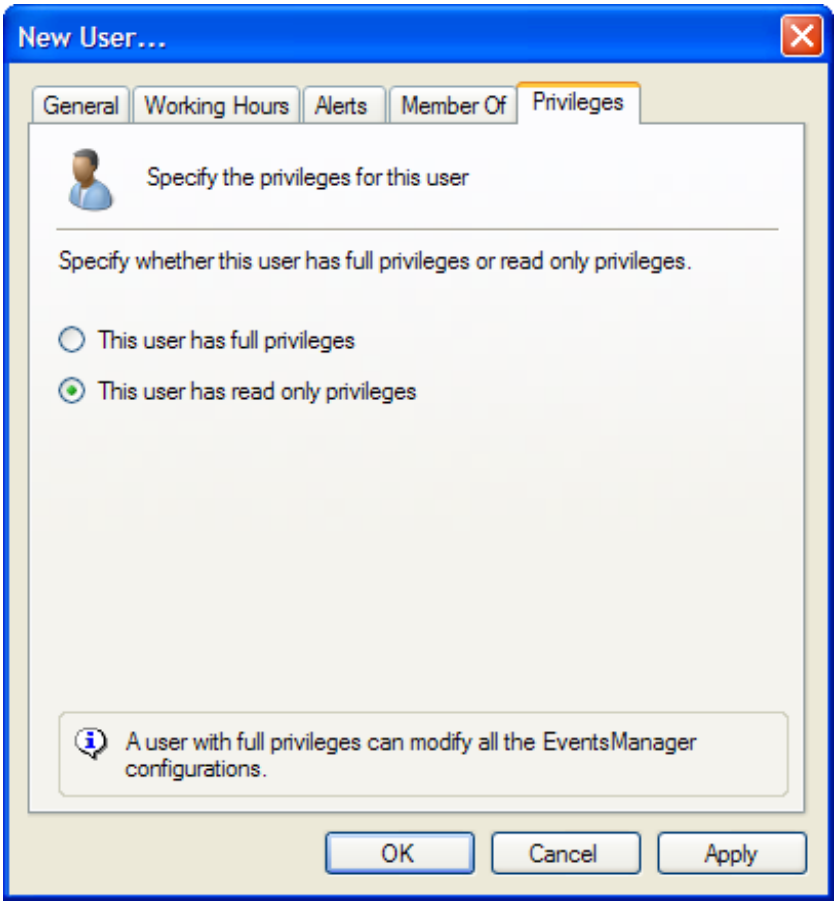
Erstellen eines neuen Benutzers

So erstellen Sie einen Benutzer:

1. Klicken Sie auf den Reiter **Configuration** ▸ **Options**.
2. Erweitern Sie die Struktur des Knotens **Users and Groups**.
3. Klicken Sie mit der rechten Maustaste auf den Unterknoten **Users** und wählen Sie im Kontextmenü **Create user**.

4. Legen Sie über die Reiter **General** (Allgemein), **Working Hours** (Geschäftszeiten), **Alerts** (Warnungen) and **Member of** (Mitglied von) alle erforderlichen Einstellungen fest.

Hinweis: Weitere Informationen hierzu erhalten Sie in diesem Kapitel unter „Konfigurieren des Administratorkontos von GFI EventsManager“.



Screenshot 136 – Zugriffsrechte für neue Benutzer

5. Klicken Sie auf den Reiter **Privileges**. Durch Auswahl von **This user has full privileges** können Sie festlegen, dass der neue Benutzer Vollzugriffsrechte erhalten soll. Bei Auswahl von **This user has read only privileges** ist ihm nur der Lesezugriff möglich.

6. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen fertig zu stellen.

Ändern von Benutzereigenschaften

So ändern Sie die Eigenschaften eines Benutzers:

1. Klicken Sie im linken Fensterbereich auf den Unterknoten **Users**.

2. Klicken Sie mit der rechten Maustaste auf den zu bearbeitenden Benutzer und wählen Sie im Kontextmenü **Properties**.

3. Führen Sie die gewünschten Änderungen durch, und klicken Sie auf die Schaltfläche **OK**, um die Einstellungen fertig zu stellen.

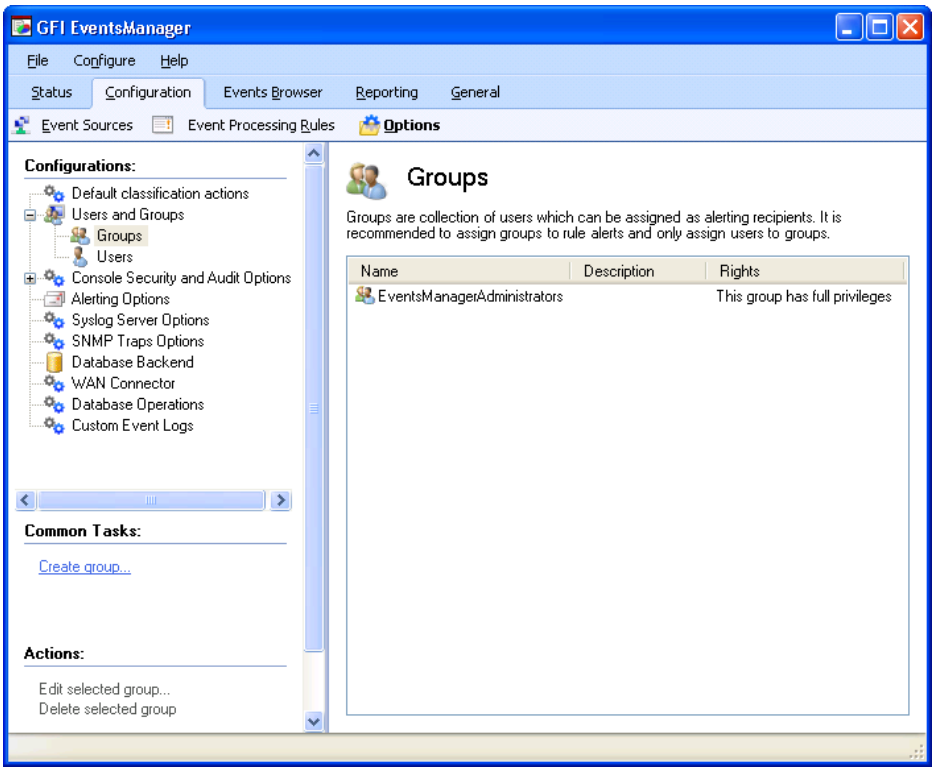
Löschen von Benutzern

So löschen Sie einen Benutzer:

1. Klicken Sie im linken Fensterbereich auf den Unterknoten **Users**.

2. Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf den zu löschenden Benutzer und wählen Sie im Kontextmenü **Delete**.

Konfigurieren einer Benutzergruppe

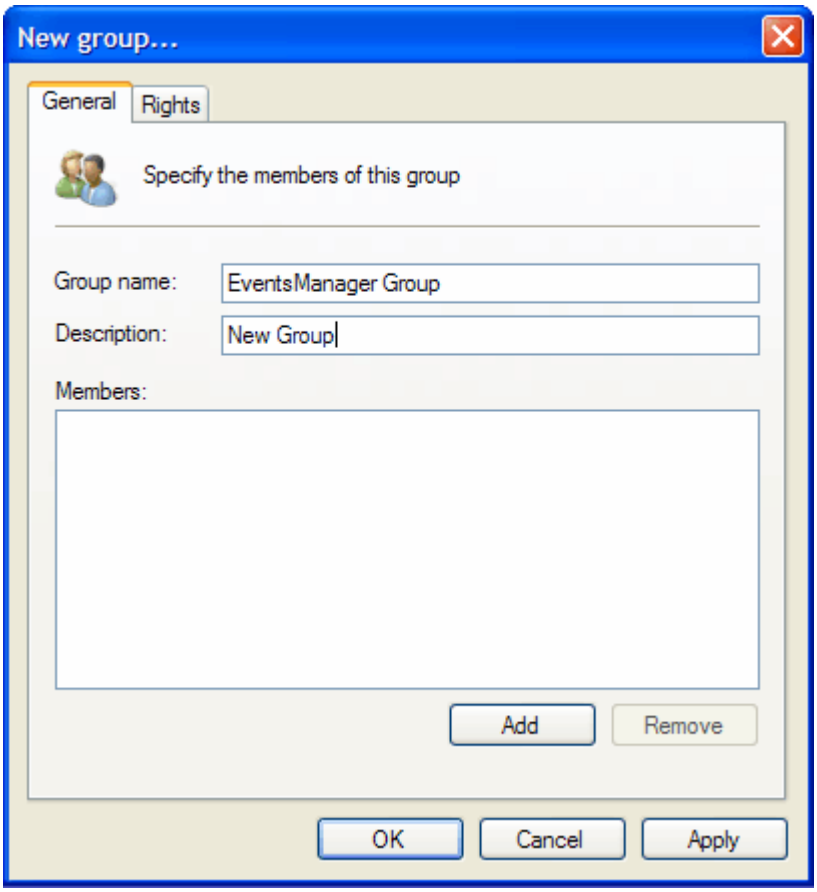


Screenshot 137 –Konfigurierung von Gruppen

1. Klicken Sie auf den Reiter **Configuration** ▸ **Options**.

2. Erweitern Sie die Struktur des Knotens **Users and Groups**.

3. Klicken Sie mit der rechten Maustaste auf den Unterknoten **Groups** und wählen Sie im Kontextmenü **Create group**.



Screenshot 138 – Einrichtung einer neuen Gruppe

4. Geben Sie der Gruppe einen Namen.

5. Klicken Sie auf die Schaltfläche **Add**, um der Gruppe Benutzer hinzuzufügen.

6. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen fertig zu stellen.

Ändern von Eigenschaften einer Benutzergruppe

So ändern Sie die Eigenschaften einer Benutzergruppe:

1. Klicken Sie im linken Fensterbereich auf den Knoten **Groups**.

2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf die zu bearbeitende Gruppe und wählen Sie im Kontextmenü **Properties**.

3. Führen Sie die gewünschten Änderungen durch, und klicken Sie auf die Schaltfläche **OK**, um die Einstellungen zu speichern.

Löschen von Benutzergruppen

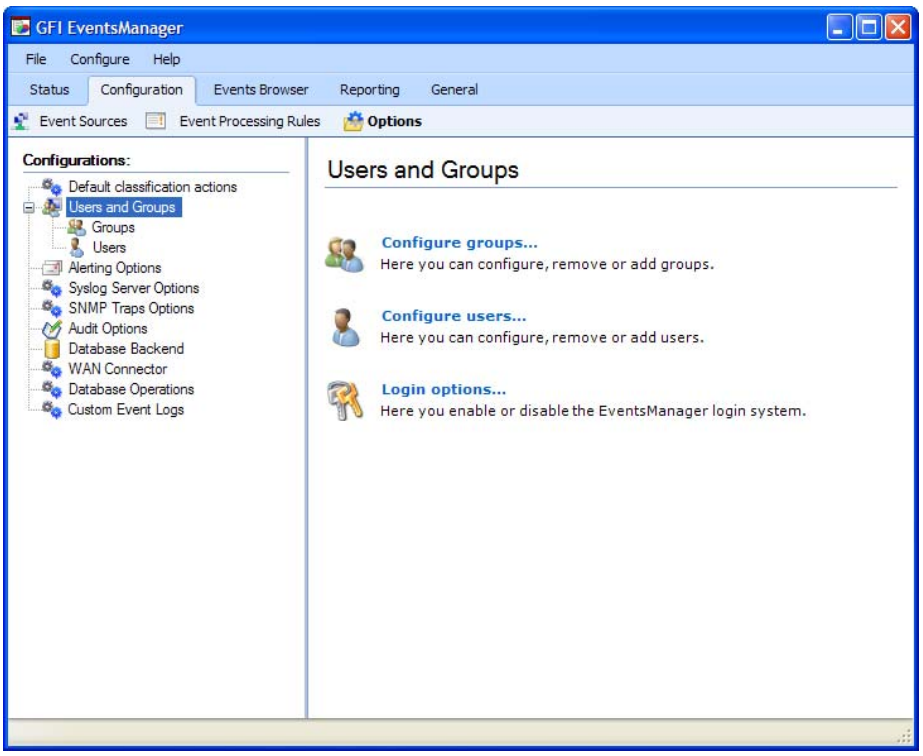
So löschen Sie eine Benutzergruppe:

1. Klicken Sie im linken Fensterbereich auf den Knoten **Groups**.

2. Klicken Sie im rechten Fenster mit der rechten Maustaste auf die zu löschende Gruppe und wählen Sie im Kontextmenü **Delete**.

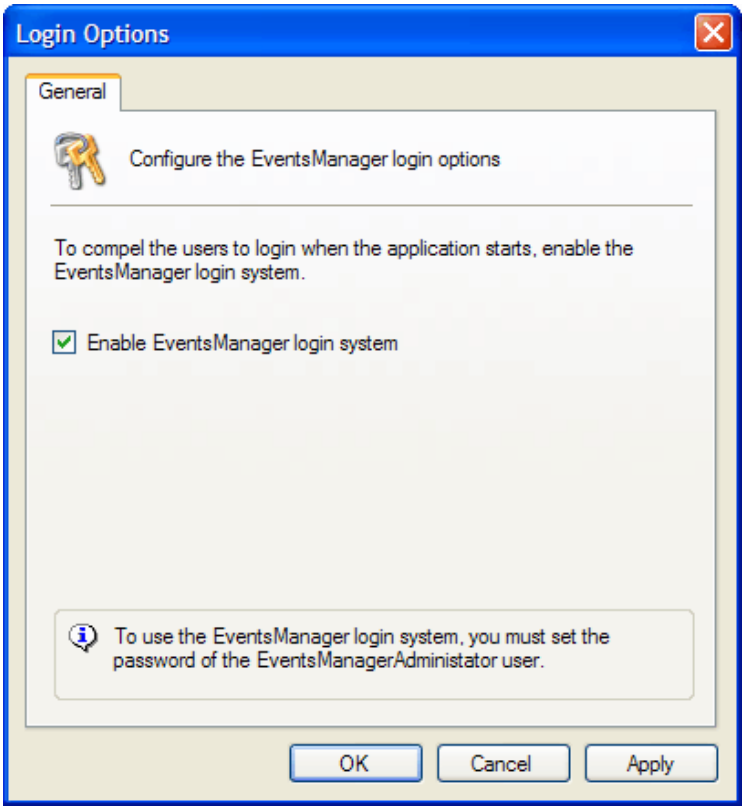
Aktivieren/Deaktivieren der Anmeldung bei GFI EventsManager

1. Klicken Sie auf den Reiter **Configuration** ▸ **Options**.



Screenshot 139 – Festlegung der Anmeldeoptionen

2. Klicken Sie im linken Fensterbereich auf den Knoten **Users and Groups** und wählen Sie rechten Fensterbereich die Option **Login options**, um die Anmeldeoptionen festzulegen.


Login Options
General
Configure the EventsManager login options
To compel the users to login when the application starts, enable the EventsManager login system.
Enable EventsManager login system
To use the EventsManager login system, you must set the password of the EventsManagerAdministator user.
OK
Cancel
Apply

Screenshot 140 – Aktivierung der Benutzeranmeldung

3. Soll GFI EventsManager erst nach Angabe von Anmelde-informationen starten, wählen Sie die Option **Enable EventsManager login system**.

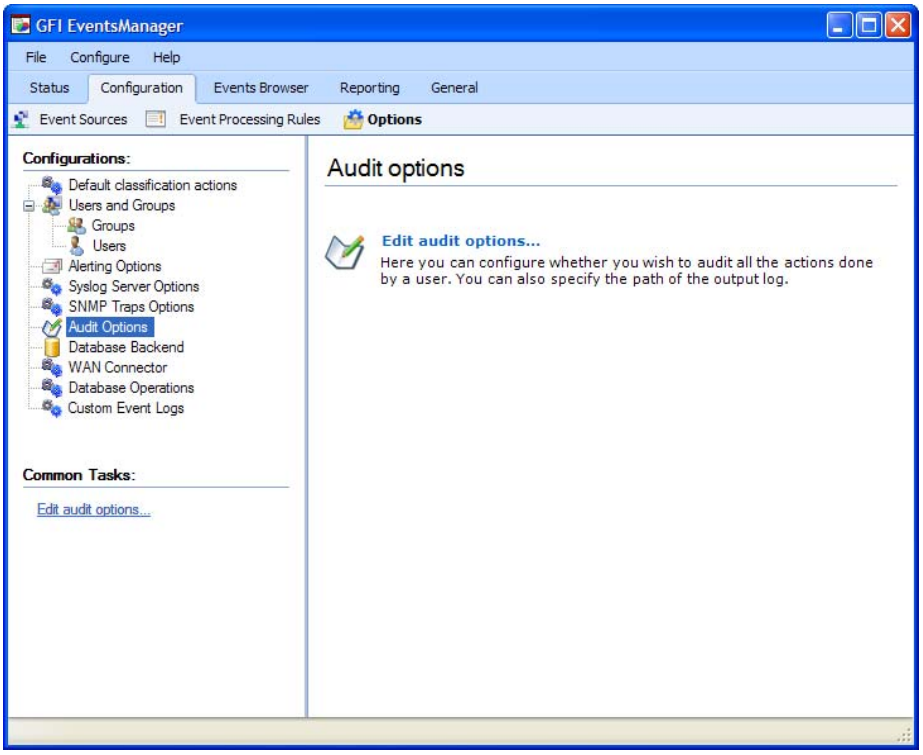
4. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen fertig zu stellen.

Hinweis 1: Bei Auswahl dieser Option muss jeder GFI EventsManager-Benutzer zum Aufruf der Verwaltungskonsole seine Anmeldeinformationen angeben.

Hinweis 2: Der Umfang des Zugriffs (Vollzugriff oder lediglich Lesezugriff) erfolgt gemäß den Rechten, die über den Reiter **Privileges** für den jeweiligen Benutzer festgelegt worden sind.

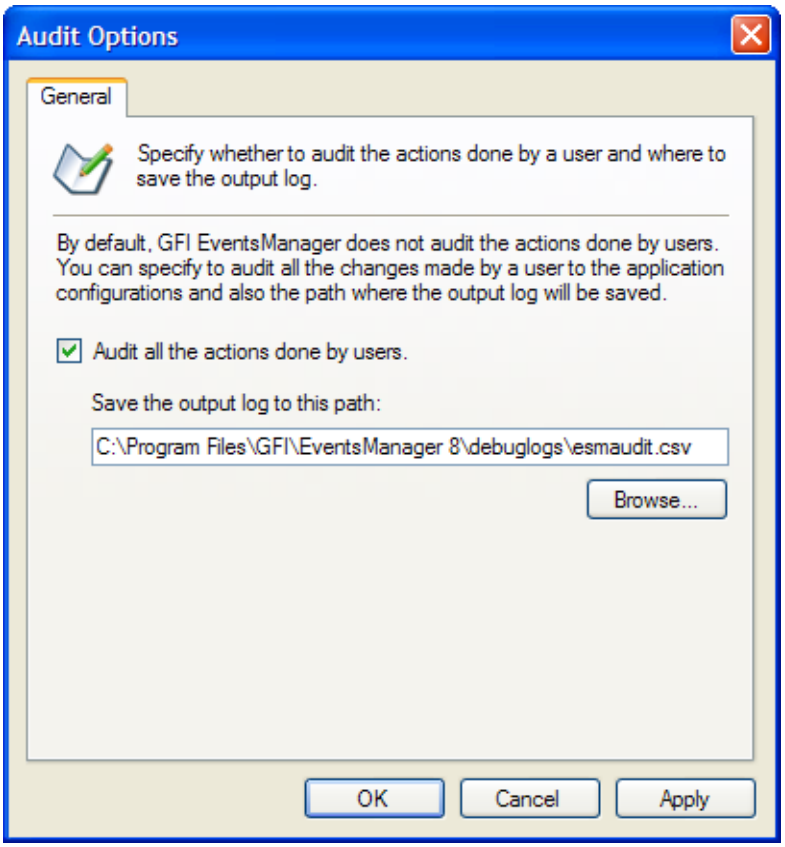
Aktivieren/Deaktivieren der Überwachung von Benutzeraktionen

1. Klicken Sie auf den Reiter **Configuration** ▸ **Options**.



Screenshot 141 – Festlegung der Überwachungsoptionen

2. Klicken Sie im linken Fensterbereich auf den Knoten **Audit Options** und wählen Sie im rechten Fensterbereich die Option **Edit audit options**.


Audit Options
General
Specify whether to audit the actions done by a user and where to save the output log.
By default, GFI EventsManager does not audit the actions done by users. You can specify to audit all the changes made by a user to the application configurations and also the path where the output log will be saved.
Audit all the actions done by users.
Save the output log to this path:
C:\Program Files\GFI\EventsManager 8\debuglogs\esmaudit.csv
Browse...
OK
Cancel
Apply

Screenshot 142 – Überwachungsoptionen

3. Wählen Sie die Option **Audit all the actions done by users**, damit sämtliche von Benutzern durchgeführte Aktionen überwacht und protokolliert werden. Geben Sie den Speicherort der Protokolldatei an.

4. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen fertig zu stellen.

Weiterführende Optionen

Befehlszeilen-Tools

GFI EventsManager bietet drei Befehlszeilen-Tools für den Export und Import von Daten:

- Exportdata.exe: Exportiert Daten aus einer Datenbank von GFI EventsManager 8 mit Hilfe des Moduls **Database Operations**.
- Importdata.exe: Importiert Daten in eine Datenbank von GFI EventsManager 8 mit Hilfe des Moduls **Database Operations**.
- Importsettings.exe: Importiert Konfigurationseinstellungen aus einem Ordner oder einer konfigurationsspezifischen Export-Datei (.esmbkp). Dieses Tool dient vorrangig der Wiederherstellung zuvor gesicherter Einstellungen.

Exportdata.exe

Mit diesem Tool werden Daten aus der GFI EventsManager-Datenbank in eine Binärdatei exportiert.

Verwendung:

exportdata.exe *<Parameterangaben>*

Parameter	Erforderlich/ optional	Beschreibung
/folder: <Pfad und Ordnername>	Erforderlich	Gibt den Ordner zur Speicherung der Datendatei an.
/period: <Stundenanzahl>	Optional	Exportiert Ereignisse, die älter sind als angegeben (in Stunden). Standard: 168 Stunden/7 Tage.
/password: Datei-Passwort	Optional	Legt ein Passwort für die Verschlüsselung fest.
/delete	Optional	Löscht die Ereignisse nach dem Export.
/movetodb:<Datenbank-Name>	Optional	Verschiebt Ereignisse in eine andere Datenbank auf demselben Server. Bei Nichtangabe des Namens wird die Backup-Datenbank gewählt.

Hinweis: Parameter mit Leerzeichen müssen in doppelten Anführungszeichen (") stehen.

Beispiel:

Exportdata.exe /folder:c:\exportfiles /period:240 /password:aip112sK

Bei diesem Beispiel erfolgt der Datenexport wie folgt:

- In einen Ordner Verzeichnis mit dem Namen „exportfiles“ auf Laufwerk „c:\“.
- Es werden Ereignisse exportiert, die älter als 240 Stunden/10 Tage sind.
- Die Daten werden mit dem Passwort „aip112sK“ geschützt.

Importdata.exe

Mit diesem Tool werden in Binärdateien gesicherte Daten in die GFI EventsManager-Datenbank importiert.

Verwendung:

importdata.exe <*Parameterangaben*>

Parameter	Erforderlich/ optional	Beschreibung
/folder:<Pfad und Ordnername>	Erforderlich	Gibt den Ordner zur Speicherung der Datendatei an.
/password:<*Datei-Passwort*>	Optional	Gibt das Passwort zur Freigabe der Datei an, sofern erforderlich.
/dbserver:<IP-Adresse des Datenbank-Servers>	Optional	Gibt den Server mit der Ziel-Datenbank an. Bei Nichtangabe werden die in GFI EventsManager definierten Datenbankinformationen verwendet.
/dbname:<Datenbank-Name>	Optional	Gibt den Namen der Ziel-Datenbank an. Bei Nichtangabe wird der in GFI EventsManager definierte Datenbank-Name verwendet.
/dbuser:<Benutzer-name>	Optional	Gibt den Benutzernamen zur Herstellung der Datenbank-Verbindung an. Bei Nichtangabe wird die Windows-Authentifizierung verwendet.
/dbpass:<Passwort>	Optional	Gibt das Passwort für die Verbindungsherstellung mit dem Ziel-Server/der Ziel-Datenbank an. Bei Nichtangabe wird das Passwort ignoriert.

Hinweis: Parameter mit Leerzeichen müssen in doppelten Anführungszeichen (") stehen.

Beispiel:

importdata.exe /folder:c:\exportfiles /password:aip112sK /dbserver:192.168.3.55 /dbname:mainesmdb /dbuser:sa /dbpass:sapwd

Bei diesem Beispiel erfolgt der Datenimport wie folgt:

- Aus einem Ordner mit dem Namen „exportfiles“ auf Laufwerk „c:\“.
- Die Daten werden mit dem Passwort „aip112sK“ freigegeben.
- Es erfolgt die Speicherung in der Datenbank auf dem Server mit der IP-Adresse 192.168.3.55. Der Datenbank-Name lautet „mainesmdb“ und folgende Anmeldeinformationen sind erforderlich: Benutzername: „sa“ und Passwort „sapwd“.

Importsettings.exe

Mit diesem Tool können zuvor exportierte Konfigurationseinstellungen von GFI EventsManager importiert werden.

Verwendung:

importsettings.exe *<Parameterangaben>*

Parameter	Erforderlich/ optional	Beschreibung
/operation:<*Vorgang*>	Erforderlich	Gibt den durchzuführenden Vorgang an (Import eines Verzeichnisses (importfolder) oder einer Datei (importfile))
/destination:<Zielordner>	Optional	Gibt den Zielordner an, in den die Konfigurationsdaten importiert werden sollen.
/Sourcefile: <*Dateiname*>	Optional	Gibt den Namen der Datei mit den exportierten Konfigurationsdaten von GFI EventsManager an.
/Sourcefolder: <*Ordnername/Pfad*>	Optional	Gibt den Namen des Ordners mit den exportierten Konfigurationsdaten von GFI EventsManager an.

Hinweis: Parameter mit Leerzeichen müssen in doppelten Anführungszeichen (") stehen.

Beispiel:

importdata.exe /operation:importfolder: /destination: c:\esm\data /sourcefolder: c:\esm\old /

Bei diesem Beispiel erfolgt der Datenimport wie folgt:

- Per Vorgang „importfolder“ werden Konfigurationsdaten aus dem Ordner „c:\esm\old“ in den Ordner „c:\esm\data“ importiert.

Anpassen von eindeutigen Kennungen (Unique Identifiers)

Die eindeutige Kennung einer Instanz von GFI EventsManager lässt sich ebenfalls per Befehlszeile verändern. Hierdurch können Sie dieselben Konfigurationseinstellungen importieren, ohne doppelte Instanzkennungen zu erhalten.

Fügen Sie die folgende Option den Befehlszeilenparametern von importdata.exe hinzu, um eine neue eindeutige Kennung für eine Instanz von GFI EventsManager anzugeben.

Parameter	Erforderlich/ optional	Beschreibung
/id: *<neue ID>*	Optional	Gibt nach dem Import der Konfigurations-einstellungen die neue Kennung der Instanz von GFI EventsManager an. Dieser Parameter dient nur der Änderung der Instanz-ID. Bei Nichtangabe wird die bestehende ID beibehalten.

Lizenzierung

So überprüfen Sie die Lizenzinformationen von GFI EventsManager:

1. Klicken Sie auf den Reiter **General**.

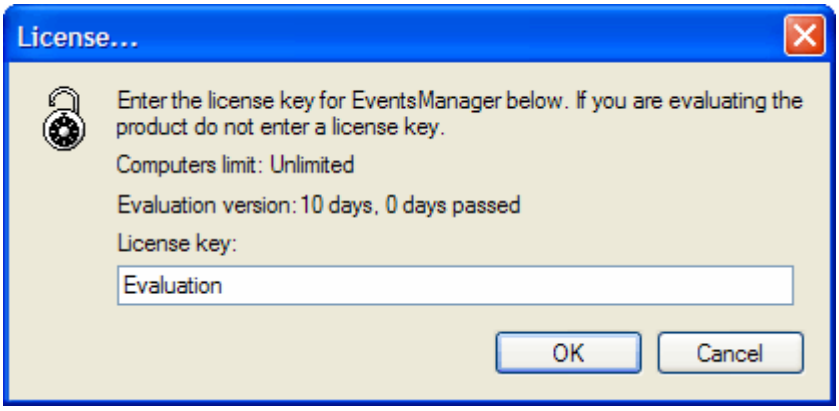
2. Klicken Sie im linken Fensterbereich auf **Licensing**. Die Lizenz-informationen werden im rechten Fensterbereich der Verwaltungs-konsole angezeigt.

Eingeben des Registrierschlüssels nach der Installation

So geben Sie den Registrierschlüssel nach der Installation ein:

1. Klicken Sie auf den Reiter **General**.

2. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf **Licensing** und wählen Sie im Kontextmenü **Edit license key…**


License…
Enter the license key for EventsManager below. If you are evaluating the product do not enter a license key.
Computers limit: Unlimited
Evaluation version: 10 days, 0 days passed
License key:
Evaluation
OK
Cancel

Screenshot 143 – Eingabe des Registrierschlüssels

3. Geben Sie den Registrierschlüssel an.

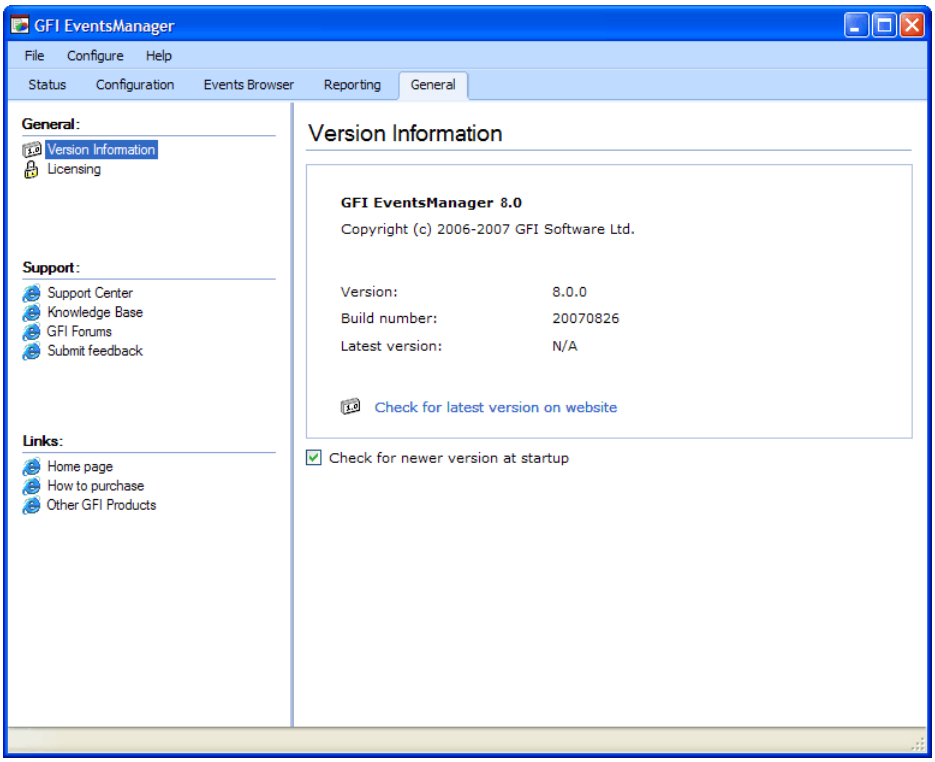
4. Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen fertig zu stellen.

Versionsinformationen

So überprüfen Sie die von Ihnen verwendete Version von GFI EventsManager:

1. Klicken Sie auf den Reiter **General**.

2. Klicken Sie im linken Fensterbereich auf **Version Information**. Die Versionsinformationen werden im rechten Fensterbereich der Verwaltungskonsole angezeigt.



Screenshot 144 – Versionsinformationen

Suchen nach neueren Builds

So suchen Sie nach neueren Builds von GFI EventsManager:

1. Klicken Sie auf den Reiter **General**.

2. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf **Version Information** und wählen Sie im Kontextmenü **Check for newer builds…**

Fehlerbehebung

Einführung

In diesem Kapitel erfahren Sie, welche Hilfsmöglichkeiten es zur Lösung von Problemen mit Ihrem GFI-Produkt gibt. Folgende Informationsquellen stehen zur Verfügung:

- Das Handbuch – die meisten Probleme lassen sich mit Hilfe dieses Handbuchs lösen
- Artikel aus der GFI Knowledge-Base
- Das Web-Forum
- Der technische Support von GFI Software

Knowledge-Base

Die Knowledge-Base von GFI hält Antworten zu den am häufigsten gestellten Fragen bereit und liefert Hinweise zur Behebung gängiger Probleme. Bei Schwierigkeiten mit Ihrem GFI-Produkt sollten Sie zunächst die zahlreichen Artikel dieser Wissensdatenbank durchsuchen. Sie bieten immer die neuesten Informationen zu Support-Fragen und Patches und können aufgerufen werden unter: http://kbase.gfi.com.

Web-Forum

Über das Web-Forum steht Ihnen der User-to-User-Support zur Verfügung. Das Forum erreichen Sie unter: http://forums.gfi.com/

Technischer Support von GFI

Sollte sich Ihr Problem nicht mit Hilfe dieses Handbuchs oder über die Knowledge-Base-Artikel lösen lassen, steht Ihnen der technische Support von GFI gerne zur Verfügung. Bitte übermitteln Sie Ihre Anfrage per Online-Formular oder kontaktieren Sie den Support telefonisch.

- **Online-Support:** Bitte füllen Sie unser Online-Support-Formular aus, das Sie auf dieser Web-Seite finden: http://support.gfi.com/supportrequestform.asp?lcode=de Folgen Sie den Anweisungen auf der Formularseite, damit Ihre Anfrage schnellstmöglich bearbeitet werden kann.
- **Telefon-Support:** Bitte informieren Sie sich auf der folgenden Web-Seite über die für Ihr Land gültige Telefonnummer des technischen Supports von GFI: http://www.gfisoftware.de/de/company/contact.htm

Hinweis: Sollten Sie unseren technischen Support kontaktieren, halten Sie bitte Ihre Customer-ID bereit. Die Customer-ID ist die Nummer Ihres Online-Kontos, die Ihnen beim ersten Registrieren Ihrer Registrierschlüssel über den GFI-Kundenbereich (http://customers.gfi.com) zugewiesen wurde.

Ihre Anfrage wird für gewöhnlich binnen 24 Stunden oder innerhalb eines Werktags beantwortet.

Benachrichtigung bei neuen Builds

Um über die neuesten Produkt-Builds Ihrer GFI-Lösung auf dem Laufenden zu bleiben, sollten Sie die entsprechende GFI-Produkt-Newslist abonnieren. Besuchen Sie hierfür: http://www.gfi.com/pages/productmailing.htm.

Index

A

Aktion 5, 6, 10, 13, 41, 55, 56, 57, 72, 75, 77, 126, 129, 132, 135, 137, 138
Aktualisierung 21
Anmeldeinformationen 47
Arbeitszeit 34, 126, 129, 131, 134, 137

B

Betriebszeit 45, 47, 126, 129, 131, 134, 137

D

Datenbank-Backend 10, 13, 29, 30, 31, 72, 91
Datenbankoperation 103, 105
demilitarisierte Zone 18, 19
DNS-Server 19, 25, 58

E

E-Mail-Warnung 6, 32, 37, 38, 55, 75
Ereignisabfrage 10, 80, 81, 85
Ereignisabfrage-Generator 10, 85
Ereignisarchivierung 6, 29, 72, 75
Ereigniskennzeichnung 82
Ereignisklassifizierung 10, 56, 72, 75, 77
Ereignisquelle 9, 12, 13, 41, 43, 44, 47, 60, 63, 126, 129, 131, 134, 137
Ereignissuche 83
Erste-Schritte-Dialog 30, 32, 37, 41
Events Browser 5, 79
Export in CSV-Dateien 83, 90

F

Filterbedingung 109, 110, 112, 114, 115

G

Geschäftszeiten 6, 32, 47

I

Installationsassistent 21

L

Lizenzierung 14, 22, 152

M

Management Information Base 11

N

Netzwerk-Warnung 7, 33, 77
Noise 13, 56, 121

R

Regel zur Ereignisverarbeitung 5, 7, 9, 10, 13, 55, 61, 63, 66, 70, 72, 73, 74, 75, 77, 121
Regelsatz 73, 122, 123, 124, 127, 130, 132, 135

S

Sicherung von Ereignissen 91
SMS-Warnung 6, 7, 32, 37
SNMP-Trap 5, 6, 7, 13, 21, 28, 68, 69, 79, 95, 99, 100, 121, 132, 135
SNMP-Trap-Server 71
SQL-Server-Audit 11, 50, 55, 79, 121, 135
Status-Monitor 93
Syslog-Meldung 7, 13, 19, 27, 64, 65, 67, 130
Syslog-Server 27, 64, 65, 66

T

Testversion 15

V

Versionsinformation 153

W

W3C-Protokoll 12, 25, 27, 55, 62, 127, 138
WAN-Connector 11
Warnung per Netzwerknachricht 38
Warnungseinstellungen 37

Windows-Ereignisprotokoll 8,
9, 12, 25, 45, 55, 57,
59, 62, 73, 121

Z

Zugriffsrecht 21